

Docket No.: 60188-609

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Kenichi KAWAGUCHI

Serial No.: : Group Art Unit:

Filed: July 03, 2003 : Examiner:

For: SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE, PROGRAM DELIVERY
METHOD, AND PROGRAM DELIVERY SYSTEM

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

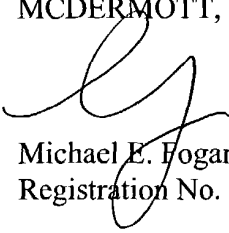
In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims the priority of:

Japanese Patent Application No. 2002-318172, filed October 31, 2002

cited in the Declaration of the present application. A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:prg
Facsimile: (202) 756-8087
Date: July 3, 2003

日本国特許庁

JAPAN PATENT OFFICE

60188-609
Kawaguchi
July 3, 2003

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2002年10月31日

出願番号

Application Number:

特願2002-318172

[ST.10/C]:

[JP2002-318172]

出願人

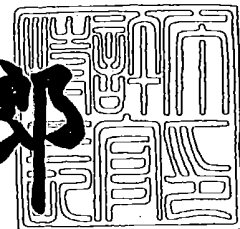
Applicant(s):

松下電器産業株式会社

2003年 4月15日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3026920

【書類名】 特許願

【整理番号】 5037740035

【提出日】 平成14年10月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 9/06

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 川口 謙一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115510

【弁理士】

【氏名又は名称】 手島 勝

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 半導体集積回路装置、並びにプログラム引き渡し方法及びそのシステム

【特許請求の範囲】

【請求項1】 バスとの間でデータの入出力を行う第1のメモリと、
前記バスとの間でデータの入出力を行う第2のメモリと、
秘密鍵を保持する秘密鍵保持部と、
外部からの前記バスへのアクセスを制御するバスポートと、
前記バスポートを経由して暗号化されたプログラムと復号プログラムとを前記第1のメモリに格納させ、前記復号プログラムと前記秘密鍵とを用いて前記暗号化されたプログラムの復号を行い、復号化されたプログラムを実行するCPUと

前記暗号化されたプログラムと前記復号プログラムとが前記第1のメモリに格納されると、前記バスポートに対して外部からのアクセスを禁止させ、前記第1及び第2のメモリへのアクセスを許可して前記暗号化されたプログラムと前記復号プログラムとの前記第1のメモリから前記第2のメモリへの転送を行い、

前記転送が終了すると、前記第1のメモリへのアクセスを禁止し、

前記復号及び前記復号化されたプログラムの実行が終了すると、前記第2のメモリへのアクセスを禁止する制御部とを備える
ことを特徴とする半導体集積回路装置。

【請求項2】 請求項1に記載の半導体集積回路装置において、

前記CPUから前記秘密鍵保持部へのアクセスを制御する秘密鍵アクセスポートをさらに備え、

前記秘密鍵アクセスポートは、

前記転送が終了すると前記秘密鍵保持部へのアクセスを許可し、前記復号化されたプログラムの実行が終了すると前記秘密鍵保持部へのアクセスを禁止するものである

ことを特徴とする半導体集積回路装置。

【請求項3】 請求項1に記載の半導体集積回路装置において、

前記CPUは、

レジスタを含み、

前記復号化されたプログラムの実行が終了すると、前記レジスタに格納されたデータを消去するものであることを特徴とする半導体集積回路装置。

【請求項4】 請求項1に記載の半導体集積回路装置において、

前記制御部は、

前記第1及び第2のメモリへのチップセレクト信号を制御することによって、前記第1及び第2のメモリへのアクセスを制御するものであることを特徴とする半導体集積回路装置。

【請求項5】 請求項1に記載の半導体集積回路装置において、

前記制御部は、

第1のフラグと第2のフラグとを格納するフラグ格納部を含み、

前記第1のフラグがセットされているときには前記第1のメモリ及び前記第2のメモリへのアクセスを許可し、前記第1のフラグがリセットされ、前記第2のフラグがセットされているときには前記第1のメモリへのアクセスを禁止し、前記第1及び第2のフラグのいずれもがリセットされているときには、前記第2のメモリへのアクセスを禁止するものであり、

前記バスポートは、

前記第1または第2のフラグのうち少なくとも1つがセットされているときに、外部からのアクセスを禁止するものであり、

前記CPUは、

前記暗号化されたプログラム及び前記復号プログラムが前記第1のメモリに入力されると前記第1のフラグ及び前記第2のフラグをセットし、前記転送が終了すると前記第1のフラグをリセットし、前記復号化されたプログラムの実行が終了すると前記第2のフラグをリセットするものであることを特徴とする半導体集積回路装置。

【請求項6】 バスとの間でデータの入出力を行う第1のメモリと、

前記バスとの間でデータの入出力を行う第2のメモリと、

前記バスと前記第1のメモリとの間に接続され、前記バスからの前記第1のメモリへのアクセスを制御する第1のメモリポートと、

前記バスと前記第2のメモリとの間に接続され、前記バスからの前記第2のメモリへのアクセスを制御する第2のメモリポートと、

秘密鍵を保持する秘密鍵保持部と、

外部からの前記バスへのアクセスを制御するバスポートと、

レジスタを有し、前記バスポートを経由して暗号化されたプログラムと復号プログラムとの前記第1のメモリへの書き込みを行い、前記復号プログラムと前記秘密鍵とを用いて前記暗号化されたプログラムの復号を行い、復号化されたプログラムの前記第2のメモリへの書き込みを行い、復号化されたプログラムを実行するCPUと、

前記第1のメモリへの書き込みが終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記第1のメモリポートに対して前記第1のメモリへの書き込みを禁止させ、前記第2のメモリポートに対して前記第2のメモリへのアクセスを許可させ、

前記復号化されたプログラムの実行が終了すると、前記CPUに対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させるとともに、前記第2のメモリポートに対して前記第2のメモリへのアクセスを禁止させる制御部とを備える

ことを特徴とする半導体集積回路装置。

【請求項7】 バスとの間でデータの入出力を行う第1のメモリと、

前記バスとの間でデータの入出力を行う第2のメモリと、

前記バスと前記第1のメモリとの間に接続され、前記バスからの前記第1のメモリへのアクセスを制御するメモリポートと、

秘密鍵を保持する秘密鍵保持部と、

外部からの前記バスへのアクセスを制御するバスポートと、

レジスタを有し、前記バスポートを経由して暗号化されたプログラムと復号プログラムとの前記第1のメモリへの書き込みを行い、前記復号プログラムと前記秘密鍵とを用いて前記暗号化されたプログラムの復号を行い、復号化されたプロ

グラムの前記第 2 のメモリへの書き込みを行い、復号化されたプログラムを実行する CPU と、

前記第 2 のメモリ上のデータを消去するメモリ初期化部を含み、前記第 1 のメモリへの書き込みが終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記メモリポートに対して前記第 1 のメモリへの書き込みを禁止させ、

前記復号化されたプログラムの実行が終了すると、前記 CPU に対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させ、前記メモリ初期化部に対して前記第 2 のメモリ上のデータを消去させるものである

ことを特徴とする半導体集積回路装置。

【請求項 8】 バスとの間でデータの入出力を行う第 1 のメモリと、

前記バスとの間でデータの入出力を行う第 2 のメモリと、

秘密鍵を保持する秘密鍵保持部と、

復号鍵を保持する復号鍵保持部と、

外部からの前記バスへのアクセスを制御するバスポートと、

レジスタを含み、前記バスポートを経由して暗号化された復号鍵と復号鍵復号プログラムとを前記第 1 のメモリへ格納する第 1 の格納を行い、前記復号鍵復号プログラムと前記秘密鍵とを用いて前記暗号化された復号鍵を復号する第 1 の復号を行い、復号化された復号鍵の前記復号鍵保持部への書き込みを行い、暗号化されたプログラムと復号プログラムとを前記第 1 のメモリへ格納する第 2 の格納を行い、前記復号プログラムと前記復号化された復号鍵とを用いて前記暗号化されたプログラムを復号する第 2 の復号を行い、復号化されたプログラムを実行する CPU と、

前記第 1 のメモリへの前記第 1 の格納が終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記第 1 のメモリ及び前記第 2 のメモリへのアクセスを許可して前記暗号化された復号鍵と前記復号鍵復号プログラムとの前記第 1 のメモリから前記第 2 のメモリへの転送を行い、

この転送が終了すると、前記秘密鍵保持部へのアクセスを許可し、前記第 1 の

メモリへのアクセスを禁止し、

前記第1の復号が終了すると、前記CPUに対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させるとともに、前記第2のメモリへのアクセスを禁止し、前記第1のメモリへのアクセスを許可し、前記バスポートに対して外部からの前記バスへのアクセスを許可し、

前記第1のメモリへの前記第2の格納が終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記第2のメモリへのアクセスを許可して前記暗号化されたプログラムと前記復号プログラムとの前記第1のメモリから前記第2のメモリへの転送を行い、

この転送が終了すると、前記復号鍵保持部へのアクセスを許可し、前記第1のメモリへのアクセスを禁止し、

前記第2の復号と前記復号化されたプログラムの実行が終了すると、前記CPUに対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させ、前記第2のメモリへのアクセスを禁止する制御部とを備える

ことを特徴とする半導体集積回路装置。

【請求項9】 第1の装置と第2の装置との間でプログラムの引き渡しを行うプログラム引き渡し方法であって、

前記第2の装置から前記第1の装置への公開鍵の転送を行うステップと、

前記第2の装置にその外部から復号プログラムを転送するステップと、

前記第1の装置において、前記公開鍵を用いて、前記プログラムの暗号化を行い、暗号化されたプログラムを前記第2の装置に転送するステップと、

前記第2の装置において、前記公開鍵に対応する秘密鍵と前記復号プログラムとを用いて、前記暗号化されたプログラムを復号するステップとを備える

ことを特徴とするプログラム引き渡し方法。

【請求項10】 第1の装置と第2の装置との間でプログラムの引き渡しを行うプログラム引き渡し方法であって、

前記第2の装置から前記第1の装置への公開鍵の転送を行うステップと、

前記第1の装置において、前記公開鍵を用いて、復号鍵の暗号化を行い、暗号

化された復号鍵を前記第 2 の装置に転送するステップと、

前記第 2 の装置において、前記公開鍵に対応する秘密鍵を用いて、前記暗号化された復号鍵を復号するステップと、

前記第 1 の装置において、前記復号鍵に対応する暗号鍵を用いて、前記プログラムの暗号化を行い、暗号化されたプログラムを前記第 2 の装置に転送するステップと、

前記第 2 の装置において、復号化された復号鍵を用いて、前記暗号化されたプログラムを復号するステップとを備える
ことを特徴とするプログラム引き渡し方法。

【請求項 1 1】 第 1 の装置と第 2 の装置とを備え、前記第 1 の装置と前記第 2 の装置との間でプログラムの引き渡しを行うプログラム引き渡しシステムであって、

前記第 1 の装置は、

前記プログラムを公開鍵を用いて暗号化し、その暗号化したプログラムを前記第 2 の装置への転送を行うものであり、

前記第 2 の装置は、

前記第 1 の装置によって暗号化されたプログラムを、前記公開鍵に対応する秘密鍵と、当該第 2 の装置の外部から転送された復号プログラムとを用いて復号するものである

ことを特徴とするプログラム引き渡しシステム。

【請求項 1 2】 第 1 の装置と第 2 の装置とを備え、前記第 1 の装置と前記第 2 の装置との間でプログラムの引き渡しを行うプログラム引き渡しシステムであって、

前記第 1 の装置は、

公開鍵を用いて、復号鍵を暗号化し、暗号化した復号鍵を前記第 2 の装置への転送を行い、

前記復号鍵に対応する暗号鍵を用いて、前記プログラムを暗号化し、暗号化したプログラムを前記第 2 の装置への転送を行うものであり、

前記第 2 の装置は、

前記公開鍵に対応する秘密鍵を用いて、前記第 1 の装置によって暗号化された復号鍵を復号し、復号化された復号鍵を用いて、前記第 1 の装置によって暗号化されたプログラムを復号するものであることを特徴とするプログラム引き渡しシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号化されたプログラムを復号して実行する機能を有する情報機器等に搭載される半導体 L S I に関する。また、プログラムを暗号化してプログラム所有者側の機器からプログラム使用者側の機器へ引き渡しす処理システム及びその方法に関する。

【0002】

【従来の技術】

近年、プログラムの書き換えが可能な、またはユーザプログラムの実行が可能な情報機器の普及に伴い、ソフトウェアの違法なコピーを防止する仕組みが考えられている。プログラムを暗号化して配信する方式においては、暗号化されたプログラムを復号するプログラム（以下、「復号プログラム」という）をコピーされないような工夫がなされている。例えば、復号プログラムを外部から読み出すことができない L S I 内部のメモリに配置し、さらに、復号化されたプログラムを外部から読み出すことができないようにしている（例えば、特許文献 1 参照）。

【0003】

図 1 8 は、暗号化されたプログラムを実行する従来の半導体集積回路装置を示すブロック図である。

【0004】

図 1 8 に示す半導体集積回路装置 1 は、CPU 3 と、内部バス 7 を介してデータの入出力を行う内蔵 ROM 4 及び内蔵 RAM 5 と、外部バス 2 を通じて外部とのデータの入出力を制御するバスポート 6 と、CPU 3 に I O バス 8 を介して接続された I O ポート 9 と、内蔵 RAM 5 を制御するメモリポート 1 0 と、メモリ

ポート10を制御する制御レジスタ11とを有している。

【0005】

暗号化されたプログラムを復号する復号プログラムは内蔵ROM4に格納されている。暗号化されたプログラムは内蔵RAM5に読み込まれ、復号プログラムによって復号される。復号化されたプログラムは内蔵RAM5に書き出される。内蔵RAM5に書き出された復号化されたプログラムは制御レジスタ11からの制御によって、メモリポート10から外部へ読み出されることを防ぐ。

【0006】

【特許文献1】 特開平8-30558号公報

【0007】

【発明が解決しようとする課題】

しかしながら、上記のように、復号プログラムをLSI内部に保持するため、不揮発性メモリをLSIに内蔵しなければならない。したがって、LSIに要するコストが高くなる。

【0008】

また、悪意のあるプログラムを暗号化してLSI内部に読み込ませ、プログラムを実行するときに、そのプログラムが復号プログラムを外部に転送することによって、復号プログラムがハッキングされる可能性がある。その結果、ハッキングされた復号プログラムを用いることによって、暗号化されたプログラムのハッキングが可能になる。さらに、復号プログラムを変更することはできないので、一度ハッキングされるとそのLSIは使えなくなる。

【0009】

さらに、暗号化されたプログラムを転送する側で暗号プログラムや暗号強度の選択ができないといった問題が生じている。

【0010】

そこで、本発明の目的は、コストを低減し、暗号化されたプログラムがハッキングされる可能性を低減した半導体集積回路装置を提供することである。

【0011】

【課題を解決するための手段】

上記課題を解決するために、第 1 に、本発明の請求項 1 に係る半導体集積回路装置は、バスとの間でデータの入出力を行う第 1 のメモリと、前記バスとの間でデータの入出力を行う第 2 のメモリと、秘密鍵を保持する秘密鍵保持部と、外部からの前記バスへのアクセスを制御するバスポートと、前記バスポートを経由して暗号化されたプログラムと復号プログラムとを前記第 1 のメモリに格納させ、前記復号プログラムと前記秘密鍵とを用いて前記暗号化されたプログラムの復号を行い、復号化されたプログラムを実行する CPU と、前記暗号化されたプログラムと前記復号プログラムとが前記第 1 のメモリに格納されると、前記バスポートに対して外部からのアクセスを禁止させ、前記第 1 及び第 2 のメモリへのアクセスを許可して前記暗号化されたプログラムと前記復号プログラムとの前記第 1 のメモリから前記第 2 のメモリへの転送を行い、前記転送が終了すると、前記第 1 のメモリへのアクセスを禁止し、前記復号及び前記復号化されたプログラムの実行が終了すると、前記第 2 のメモリへのアクセスを禁止する制御部とを備えるものである。

【 0 0 1 2 】

請求項 1 の発明によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【 0 0 1 3 】

また、請求項 2 の発明は、請求項 1 に記載の半導体集積回路装置において、前記 CPU から前記秘密鍵保持部へのアクセスを制御する秘密鍵アクセスポートをさらに備え、前記秘密鍵アクセスポートは、前記転送が終了すると前記秘密鍵保持部へのアクセスを許可し、前記復号化されたプログラムの実行が終了すると前記秘密鍵保持部へのアクセスを禁止するものである。

【 0 0 1 4 】

また、請求項 3 の発明は、請求項 1 に記載の半導体集積回路装置において、前記 CPU は、レジスタを含み、前記復号化されたプログラムの実行が終了すると

、前記レジスタに格納されたデータを消去するものである。

【0015】

また、請求項4の発明は、請求項1に記載の半導体集積回路装置において、前記制御部は、前記第1及び第2のメモリへのチップセレクト信号を制御することによって、前記第1及び第2のメモリへのアクセスを制御するものである。

【0016】

また、請求項5の発明は、請求項1に記載の半導体集積回路装置において、前記制御部は、第1のフラグと第2のフラグとを格納するフラグ格納部を含み、前記第1のフラグがセットされているときには前記第1のメモリ及び前記第2のメモリへのアクセスを許可し、前記第1のフラグがリセットされ、前記第2のフラグがセットされているときには前記第1のメモリへのアクセスを禁止し、前記第1及び第2のフラグのいずれもがリセットされているときには、前記第2のメモリへのアクセスを禁止するものでり、前記バスポートは、前記第1または第2のフラグのうち少なくとも1つがセットされているときに、外部からのアクセスを禁止するものであり、前記CPUは、前記暗号化されたプログラム及び前記復号プログラムが前記第1のメモリに入力されると前記第1のフラグ及び前記第2のフラグをセットし、前記転送が終了すると前記第1のフラグをリセットし、前記復号化されたプログラムの実行が終了すると前記第2のフラグをリセットするものである。

【0017】

上記課題を解決するために、第2に、本発明の請求項6に係る発明は、バスとの間でデータの入出力を行う第1のメモリと、前記バスとの間でデータの入出力を行う第2のメモリと、前記バスと前記第1のメモリとの間に接続され、前記バスからの前記第1のメモリへのアクセスを制御する第1のメモリポートと、前記バスと前記第2のメモリとの間に接続され、前記バスからの前記第2のメモリへのアクセスを制御する第2のメモリポートと、秘密鍵を保持する秘密鍵保持部と、外部からの前記バスへのアクセスを制御するバスポートと、レジスタを有し、前記バスポートを経由して暗号化されたプログラムと復号プログラムとの前記第1のメモリへの書き込みを行い、前記復号プログラムと前記秘密鍵とを用いて前

記暗号化されたプログラムの復号を行い、復号化されたプログラムの前記第2のメモリへの書き込みを行い、復号化されたプログラムを実行するCPUと、前記第1のメモリへの書き込みが終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記第1のメモリポートに対して前記第1のメモリへの書き込みを禁止させ、前記第2のメモリポートに対して前記第2のメモリへのアクセスを許可させ、前記復号化されたプログラムの実行が終了すると、前記CPUに対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させるとともに、前記第2のメモリポートに対して前記第2のメモリへのアクセスを禁止させる制御部とを備えるものである。

【0018】

請求項6の発明によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【0019】

上記課題を解決するために、第3に、本発明の請求項7に記載の発明は、バスとの間でデータの入出力を行う第1のメモリと、前記バスとの間でデータの入出力を行う第2のメモリと、前記バスと前記第1のメモリとの間に接続され、前記バスからの前記第1のメモリへのアクセスを制御するメモリポートと、秘密鍵を保持する秘密鍵保持部と、外部からの前記バスへのアクセスを制御するバスポートと、レジスタを有し、前記バスポートを経由して暗号化されたプログラムと復号プログラムとの前記第1のメモリへの書き込みを行い、前記復号プログラムと前記秘密鍵とを用いて前記暗号化されたプログラムの復号を行い、復号化されたプログラムの前記第2のメモリへの書き込みを行い、復号化されたプログラムを実行するCPUと、前記第2のメモリ上のデータを消去するメモリ初期化部を含み、前記第1のメモリへの書き込みが終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記メモリポートに対して前記第1のメモリへの書き込みを禁止させ、前記復号化されたプログラムの実行が終了する

と、前記CPUに対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させ、前記メモリ初期化部に対して前記第2のメモリ上のデータを消去させるものである。

【0020】

請求項7の発明によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【0021】

上記課題を解決するために、第4に、本発明の請求項8に記載の発明は、バスとの間でデータの入出力を行う第1のメモリと、前記バスとの間でデータの入出力を行う第2のメモリと、秘密鍵を保持する秘密鍵保持部と、復号鍵を保持する復号鍵保持部と、外部からの前記バスへのアクセスを制御するバスポートと、レジスタを含み、前記バスポートを経由して暗号化された復号鍵と復号鍵復号プログラムとを前記第1のメモリへ格納する第1の格納を行い、前記復号鍵復号プログラムと前記秘密鍵とを用いて前記暗号化された復号鍵を復号する第1の復号を行い、復号化された復号鍵の前記復号鍵保持部への書き込みを行い、暗号化されたプログラムと復号プログラムとを前記第1のメモリへ格納する第2の格納を行い、前記復号プログラムと前記復号化された復号鍵とを用いて前記暗号化されたプログラムを復号する第2の復号を行い、復号化されたプログラムを実行するCPUと、前記第1のメモリへの前記第1の格納が終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記第1のメモリ及び前記第2のメモリへのアクセスを許可して前記暗号化された復号鍵と前記復号鍵復号プログラムとの前記第1のメモリから前記第2のメモリへの転送を行い、この転送が終了すると、前記秘密鍵保持部へのアクセスを許可し、前記第1のメモリへのアクセスを禁止し、前記第1の復号が終了すると、前記CPUに対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させるとともに、前記第2のメモリへのアクセスを禁止し、前記第1のメモリへの

アクセスを許可し、前記バスポートに対して外部からの前記バスへのアクセスを許可し、前記第 1 のメモリへの前記第 2 の格納が終了すると、前記バスポートに対して外部からの前記バスへのアクセスを禁止させ、前記第 2 のメモリへのアクセスを許可して前記暗号化されたプログラムと前記復号プログラムとの前記第 1 のメモリから前記第 2 のメモリへの転送を行い、この転送が終了すると、前記復号鍵保持部へのアクセスを許可し、前記第 1 のメモリへのアクセスを禁止し、前記第 2 の復号と前記復号化されたプログラムの実行が終了すると、前記 CPU に対して前記レジスタに格納されたデータを消去させ、前記秘密鍵保持部へのアクセスを禁止させ、前記第 2 のメモリへのアクセスを禁止する制御部とを備えるものである。

【 0 0 2 2 】

請求項 8 の発明によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。さらに、暗号化されたプログラムを転送する側で暗号プログラムや暗号強度の選択することができる。

【 0 0 2 3 】

上記課題を解決するために、第 5 に、本発明の請求項 9 に係るプログラム引き渡し方法は、第 1 の装置と第 2 の装置との間でプログラムの引き渡しを行うプログラム引き渡し方法であって、前記第 2 の装置から前記第 1 の装置への公開鍵の転送を行うステップと、前記第 2 の装置にその外部から復号プログラムを転送するステップと、前記第 1 の装置において、前記公開鍵を用いて、前記プログラムの暗号化を行い、暗号化されたプログラムを前記第 2 の装置に転送するステップと、前記第 2 の装置において、前記公開鍵に対応する秘密鍵と前記復号プログラムとを用いて、前記暗号化されたプログラムを復号するステップとを備えるものである。

【 0 0 2 4 】

請求項 9 の発明によると、半導体集積回路装置の内部に復号プログラムを保持

するための不揮発性のメモリが不要でコストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【0025】

上記課題を解決するために、第6に、本発明の請求項10に係るプログラム引き渡し方法は、第1の装置と第2の装置との間でプログラムの引き渡しを行うプログラム引き渡し方法であって、前記第2の装置から前記第1の装置への公開鍵の転送を行うステップと、前記第1の装置において、前記公開鍵を用いて、復号鍵の暗号化を行い、暗号化された復号鍵を前記第2の装置に転送するステップと、前記第2の装置において、前記公開鍵に対応する秘密鍵を用いて、前記暗号化された復号鍵を復号するステップと、前記第1の装置において、前記復号鍵に対応する暗号鍵を用いて、前記プログラムの暗号化を行い、暗号化されたプログラムを前記第2の装置に転送するステップと、前記第2の装置において、復号化された復号鍵を用いて、前記暗号化されたプログラムを復号するステップとを備えるものである。

【0026】

請求項10の発明によると、半導体集積回路装置の内部に復号プログラムを保持するための不揮発性のメモリが不要でコストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。さらに、暗号化されたプログラムを転送する側で暗号プログラムや暗号強度の選択することができる。

【0027】

上記課題を解決するために、第7に、本発明の請求項11に係るプログラム引き渡しシステムは、第1の装置と第2の装置とを備え、前記第1の装置と前記第2の装置との間でプログラムの引き渡しを行うプログラム引き渡しシステムであって、前記第1の装置は、前記プログラムを公開鍵を用いて暗号化し、その暗号化したプログラムを前記第2の装置への転送を行うものであり、前記第2の装置

は、前記第 1 の装置によって暗号化されたプログラムを、前記公開鍵に対応する秘密鍵と、当該第 2 の装置の外部から転送された復号プログラムとを用いて復号するものである。

【0028】

請求項 1 1 の発明によると、半導体集積回路装置の内部に復号プログラムを保持するための不揮発性のメモリが不要でコストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【0029】

上記課題を解決するために、第 8 に、本発明の請求項 1 2 に係るプログラム引き渡しシステムは、第 1 の装置と第 2 の装置とを備え、前記第 1 の装置と前記第 2 の装置との間でプログラムの引き渡しを行うプログラム引き渡しシステムであって、前記第 1 の装置は、公開鍵を用いて、復号鍵を暗号化し、暗号化した復号鍵を前記第 2 の装置への転送を行い、前記復号鍵に対応する暗号鍵を用いて、前記プログラムを暗号化し、暗号化したプログラムを前記第 2 の装置への転送を行うものであり、前記第 2 の装置は、前記公開鍵に対応する秘密鍵を用いて、前記第 1 の装置によって暗号化された復号鍵を復号し、復号化された復号鍵を用いて、前記第 1 の装置によって暗号化されたプログラムを復号するものである。

【0030】

請求項 1 2 の発明によると、半導体集積回路装置の内部に復号プログラムを保持するための不揮発性のメモリが不要でコストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。さらに、暗号化されたプログラムを転送する側で暗号プログラムや暗号強度の選択することができる。

【0031】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照しながら説明する。

【0032】

(第1の実施形態)

図1は、本発明の第1の実施形態における半導体集積回路装置101の構成を説明するためのブロック図である。

【0033】

図1に示すように、暗号化されたプログラムが、プログラムの開発者側の機器たるPC128a(第1の装置に対応する)からPC126を介して、プログラムの使用者側へ転送される。使用者側の情報機器140内の半導体集積回路装置101(第2の装置に対応する)において、秘密鍵と復号プログラムを用いて暗号化されたプログラムを復号し実行する。

【0034】

PC128aは、プログラム開発者側の機器であり、プログラムD128aとプログラムを暗号化するための暗号プログラム128bとを保持している。

【0035】

情報機器140は、プログラム使用者側の機器であり、半導体集積回路装置101と、復号プログラムD123aを保持するフラッシュメモリ123aと、USBアップストリームポート124と、周辺機器150とを有している。なお、外部バス102によって、半導体集積回路装置101とフラッシュメモリ123aとUSBアップストリームポート124とが接続されている。

【0036】

半導体集積回路装置101は、CPU103aと、内蔵RAM104(第1のメモリに対応する)及び105(第2のメモリに対応する)と、公開鍵格納レジスタ106と、秘密鍵格納レジスタ107と、秘密鍵アクセスポート108aと、バスポート110aと、セキュリティコントローラ111aと、I/Oポート122とを有している。なお、内部バス109は、図示するように接続されている。

【0037】

CPU103aは、汎用レジスタコントローラ119aと汎用レジスタ120aとを有している。

【0038】

セキュリティコントローラ111aは、プログラム復号実行フラグ112F（第2のフラグに対応する）及びRAMコピーフラグ113F（第1のフラグに対応する）とを格納するフラグ格納部113aと、チップセレクトディスパッチャ114aと、DMA118aとを有している。

【0039】

以下に、各要素の内容及び動作について具体的に説明する。

【0040】

外部バス102は、公開鍵格納レジスタ106に格納された公開鍵のパソコン128aへの転送や、その公開鍵と暗号プログラムD128bとを用いて暗号化されたプログラムの半導体集積回路装置101への転送に用いられるものである。

【0041】

CPU103aは、内蔵RAM104や105、またはフラッシュメモリ123a上に格納されたプログラムによって動作する。通常のプログラムを動作させるほか、暗号化されたプログラムの復号や復号化されたプログラムを実行する。また、外部から入力される暗号化されたプログラムや復号プログラムD123aを内蔵RAM104に転送する。

【0042】

内蔵RAM104は、通常時、すなわち、復号プログラムD123a、復号化されたプログラムのいずれもが実行されていないときに使用されるメモリである。公開鍵と暗号プログラムD128bとを用いて暗号化されたプログラムを復号して実行する場合について説明する。まず、バスポート110aが外部バス102と内部バス109とを接続した状態で、CPU110aによって、暗号化されたプログラムとフラッシュメモリ123a内の復号プログラムD123aとが内蔵RAM104に転送される。次に、バスポート110aが外部バス102と内部バス109とを分離してから、DMA118aによって、暗号化されたプログラムと復号プログラムD123aとが内蔵RAM104から内蔵RAM105に転送される。その後は、復号されたプログラムの実行が終了するまでの間、セキ

セキュリティコントローラ111aによって、内部バス109から内蔵RAM104へのアクセスが禁止される。

【0043】

内蔵RAM105は、復号プログラムD123aの実行時、及び復号化されたプログラムの実行時に使用される。暗号化されたプログラムを復号して実行する場合について説明する。バスポート110aが外部バス102と内部バス109とを分離した後に、DMA118aによって、暗号化されたプログラムと復号プログラムD123aとが内蔵RAM104から内蔵RAM105に転送される。また、バスポート110aが外部バス102と内部バス109とを接続している状態では、セキュリティコントローラ111aによって、内部バス109から内蔵RAM105へのアクセスが禁止される。したがって、内蔵RAM105に一時的に記憶される復号化されたプログラムや、復号処理の実行途中のデータが外部から観測されることはない。

【0044】

公開鍵格納レジスタ106は、公開鍵を格納した読み出し専用のレジスタである。公開鍵は、半導体集積回路装置101の外部にあるパソコン128aに転送され、暗号プログラムD128bによってプログラムD128aを暗号化する際に用いられる鍵である。

【0045】

秘密鍵格納レジスタ107は、秘密鍵を格納した読み出し専用のレジスタである。秘密鍵は、復号プログラムD123aによって暗号化されたプログラムを復号する際に用いられる鍵である。

【0046】

秘密鍵アクセスポート108aは、RAMコピーフラグ113Fがリセットされている間にのみ、CPU103aが秘密鍵格納レジスタ107から秘密鍵を読み出すことを可能にする。すなわち、復号プログラムD123aが開始され、内蔵RAM104から内蔵RAM105への暗号化されたプログラムと復号プログラムD123aの転送が完了し、RAMコピーフラグ113Fがリセットされて、その後プログラムを復号している間と復号化されたプログラムを実行している

間にのみ、CPU103aが秘密鍵格納レジスタ107から秘密鍵を読み出すことを可能にし、それ以外の場合は秘密鍵の読み出しを禁止する。

【0047】

内部バス109は、半導体集積回路装置101内部におけるプログラムやデータの転送に使用される。

【0048】

バスポート110aは、プログラム復号実行フラグ112F、RAMコピーフラグ113Fのうちの少なくとも1つがセットされているときに、内部バス109と外部バス102とを分離する。このため、暗号化されたプログラムと復号プログラムD123aの転送中、復号プログラムD123aや復号化されたプログラムの実行中において、内部バス109及び内蔵RAM105が外部から観測されることがない。その他の場合は内部バス109と外部バス102とを接続する。

【0049】

セキュリティコントローラ111aは、プログラム復号実行フラグ112F及びRAMコピーフラグ113Fを保持するフラグ格納部113a、チップセレクトディスパッチャ114a、DMAコントローラ118（以下、「DMA」という）を内蔵する。そして、暗号プログラムD128bと公開鍵格納レジスタ106に格納された公開鍵によって暗号化されたプログラムを復号し、復号化されたプログラムを実行する際に、バスポート110a、秘密鍵アクセスポート108a、チップセレクト信号116S及び117S、汎用レジスタコントローラ119aの制御を行うものである。

【0050】

暗号プログラムD128bによって暗号化されたプログラムを復号して実行する場合について説明する。まず、バスポート110aが外部バス102と内部バス109とを接続した状態で、CPU103aによって、暗号化されたプログラム及び復号プログラムD123aが内蔵RAM104に転送されると、次に、バスポート110aが外部バス102と内部バス109とを分離する。次に、チップセレクトディスパッチャ114aはチップセレクト信号116S及び117S

をアサートさせて、DMA118aによって暗号化されたプログラム及び復号プログラムD123aを内蔵RAM104から内蔵RAM105に転送させる。転送が終了すると、チップセレクトディスパッチャ114aはチップセレクト信号116Sをネゲートし、その後は、CPU103aの制御に移る。そして、CPU103aにおいてプログラムが復号され、復号化されたプログラムの実行が終了するとチップセレクトディスパッチャ114aに終了通知がなされる。通知を受けるとチップセレクトディスパッチャ114aはチップセレクト信号117Sをネゲートし、汎用レジスタコントローラ119aに汎用レジスタ120aを初期化させ、CPU103aからのチップセレクト信号115Sをチップセレクト信号116Sとして出力する。その後、バスポート110aは内部バス109と外部バス102とを接続する。

【0051】

プログラム復号実行フラグ112Fは、復号プログラムD123aの開始時にCPU103aからセットされ、復号化されたプログラムの実行終了時にCPU103aからリセットされる。復号プログラムD123aが開始され、内蔵RAM104から内蔵RAM105への暗号化されたプログラムと復号プログラムD123aの転送が完了し、RAMコピーフラグ113Fがリセットされる。その後、暗号化されたプログラムを復号している間と復号化されたプログラムが実行されている間は、内蔵RAM104へのアクセスが禁止され、内蔵RAM105及び秘密鍵格納レジスタ107へのアクセスを可能にする。プログラム復号実行フラグ112Fがリセットされると、内蔵RAM105及び秘密鍵格納レジスタ107へのアクセスが禁止される。

【0052】

RAMコピーフラグ113Fは、復号プログラムD123aの開始時にCPU103aからセットされ、内蔵RAM104から内蔵RAM105へのデータ転送の終了時にリセットされる。内蔵RAM104及び105はメモリマップ上は同一なので、通常は双方へのチップセレクトが同時にアサートされることはない。ただし、暗号化されたプログラムなどを内蔵RAM105に転送するために、内蔵RAM104から内蔵RAM105への転送時にRAMコピーフラグ113

Fをセットすることで、内蔵RAM104、105それぞれへの、チップセレクトディスパッチャ114aからのチップセレクト信号116S、117Sをそれぞれアサートする。

【0053】

チップセレクトディスパッチャ（以下、「CSディスパッチャ」とする）114aは、RAMコピーフラグ113Fがセットされているとき、チップセレクト信号116S及び117Sをとともにアサートする。これにより、DMA118aによる内蔵RAM104から内蔵RAM105への暗号化されたプログラムと復号プログラムD123aの転送を可能にする。プログラム復号実行フラグ112Fがセットされ、かつRAMコピーフラグ113Fがリセットされているとき、チップセレクト信号116Sをネゲートにするとともにチップセレクト信号115Sをチップセレクト信号117Sとして転送する。これにより、暗号化されたプログラムの復号時、復号化されたプログラムの実行時に内蔵RAM105へのアクセスを可能にする。いずれにもあてはまらないとき、チップセレクト信号115Sをチップセレクト信号116Sとして転送するとともにチップセレクト信号117Sをネゲートする。これにより、通常時、すなわち、復号プログラムD123a、復号化されたプログラムのいずれもが実行されていないとき、内蔵RAM105へのアクセスを禁止する。

【0054】

チップセレクト信号115Sは、CPU103aから出力され、内蔵RAM104または内蔵RAM105にアクセスするときにアサートされる。

【0055】

チップセレクト信号116S及び117Sは、CSディスパッチャ114aから出力され、チップセレクト信号116Sは内蔵RAM104にアクセスするときにアサートされ、チップセレクト信号117Sは内蔵RAM105にアクセスするときにアサートされる。

【0056】

DMAコントローラ118aは、RAMコピーフラグ113Fがセットされたとき、内蔵RAM104から内蔵RAM105への暗号化されたプログラムと復

号プログラムD123aの転送を行う。なお、転送が終了するとRAMコピーフラグ113はリセットされる。

【0057】

汎用レジスタコントローラ119aは、プログラム復号実行フラグ112Fがリセットされるときに、汎用レジスタ120aをリセットする。したがって、暗号化されたプログラムの復号中、復号化されたプログラムの実行中に汎用レジスタ120aに生成されたデータが外部から観測されることはない。

【0058】

I/Oポート122は、I/Oバス121を介してCPU103aに接続されている。また、周辺機器150におけるサウンドモジュール151やビデオモジュール152などの外付けの回路と接続されている。

【0059】

フラッシュメモリ123aは、復号プログラムD123aを保持する。

【0060】

復号プログラムD123aは、半導体集積回路装置101内部の内蔵RAM104を経由して内蔵RAM105に転送され、暗号化されたプログラムを復号する際に、秘密鍵格納レジスタ107に格納された秘密鍵とともに用いられるものである。

【0061】

USBアップストリームポート124は、USBケーブル125を介してパソコン126に接続し、暗号化されたプログラムを半導体集積回路装置101に転送するのに用いられるものである。

【0062】

USBケーブル125は、パソコン126からUSBアップストリームポート124への暗号化されたプログラムの転送に用いられるものである。

【0063】

パソコン126は、パソコン128aから暗号化されたプログラムを受け取り、半導体集積回路装置101を搭載した情報機器140に暗号化されたプログラムを転送するものである。

【0064】

ネットワーク回線127は、パソコン128からパソコン126に暗号化されたプログラムを転送するために使用されるものである。

【0065】

パソコン128は、ネットワーク回線127を介してパソコン126から公開鍵格納レジスタ106に格納された公開鍵を受け取り、プログラムD128aを暗号プログラムD128bと公開鍵とを用いて暗号化し、ネットワーク回線127を介してパソコン126に転送するものである。

【0066】

プログラム128aは、暗号プログラムD128bと公開鍵格納レジスタ106に格納された公開鍵を用いて暗号化され、ネットワーク回線127、パソコン126、USBケーブル125、USBアップストリームポート124、外部バス102を介して半導体集積回路装置101に転送される。そして、半導体集積回路装置101内で、復号プログラムD123aと秘密鍵格納レジスタ107に格納された秘密鍵とを用いて復号されるものである。

【0067】

D128bは暗号プログラムであり、公開鍵格納レジスタ106に格納された公開鍵を用いてプログラムD128aを暗号化するものである。

【0068】

情報機器140は、半導体集積回路装置101、周辺機器150、フラッシュメモリ123a、及びUSBアップストリームポート124を有している。

【0069】

周辺機器150は、サウンドモジュール151、ビデオモジュール152を有しており、半導体集積回路装置101内のI/Oポート122に接続されている。

【0070】

サウンドモジュール151は、半導体集積回路装置101のI/Oポート122に接続され、データ転送の送受信、制御信号の受信を通じて、サウンドの再生、記録等を行う。

【0071】

ビデオモジュール152は、半導体集積回路装置101のI/Oポート122に接続され、データ転送の送受信、制御信号の受信を通じて、動画像の再生を行う。

【0072】

次に、図2を用いて、暗号化されたプログラムを復号してプログラムD128aを生成し、プログラムD128aを実行する手順について概説する。

【0073】

図2は、第1の実施形態における暗号化されたプログラムの復号の手順を示すフローチャートである。

【0074】

まず、ステップST201において、CPU103aは復号プログラムD123aと暗号化されたプログラムとを内蔵RAM104への転送を行う。

【0075】

次に、その転送が終了すると、ステップST202に進んで、CPU103aはプログラム復号実行フラグ112FとRAMコピーフラグ113Fとをセットする。このとき、バスポート110aは内部バス109と外部バス102との分離を行う。

【0076】

次に、その分離後、ステップST203に進んで、DMAコントローラ118aは内蔵RAM104上の復号プログラムD123aと暗号化されたプログラムとの内蔵RAM105への転送を行う。

【0077】

次に、その転送が終了すると、ステップST204に進んで、CPU103aはRAMコピーフラグ113Fをリセットする。ここから、後述するステップST206が終了するまで、CSディスパッチャ114aはチップセレクト信号116Sをアサートしない。

【0078】

次に、ステップST205に進んで、CPU103aは復号プログラムD123aを実行し、秘密鍵格納レジスタ107に格納された秘密鍵を用いて暗号化さ

れたプログラムを復号してプログラムD128aを生成する。そして、生成されたプログラムD128aを内蔵RAM105に書き込む。

【0079】

次に、ステップST206に進んで、CPU103aはプログラムD128aを実行する。

【0080】

最後に、ステップST207に進んで、CPU103aはプログラム復号実行フラグ112Fをリセットする。プログラム復号実行フラグ112Fがリセットされるとき、汎用レジスタコントローラ119aは汎用レジスタ120aをリセットする。プログラム復号実行フラグ112aがリセットされると、バスポート110aは内部バス109と外部バス102とを接続する。また、CSディスパッチャ114aはチップセレクト信号115Sをチップセレクト信号116Sとして出力し、チップセレクト信号117Sをネゲートする。

【0081】

チップセレクト信号116Sは、復号プログラムD123aが実行されプログラムD128aの生成がなされているときはアサートされないの、復号中のデータやプログラムD128aが内蔵RAM104に記憶されることはない。さらに、チップセレクト信号117Sは、バスポート110aが外部バス102と内部バス109とを接続しているときはネゲートされるので、復号中のデータやプログラムD128aが外部から観測されることはない。

【0082】

以上のように第1の実施形態によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されことなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【0083】

(第2の実施形態)

図3は第2の実施形態に係る半導体集積回路装置301の構成を説明するため

のブロック図である。

【0084】

図3に示した半導体集積回路301は、図1に示した半導体集積回路装置101と比べ、メモリポート302（第1のメモリポートに対応する）及び303（第2のメモリポートに対応する）をさらに備えている点で相違する。また、セキュリティコントローラ111bは、プログラム復号実行フラグ112Fを格納するフラグ格納部113bのみを有している点で、図1に示したセキュリティコントローラ111aと相違する。なお、その他の要素は、図1に示した要素と同様の動作を行うので、その説明は繰り返さない。

【0085】

メモリポート302は、プログラム復号実行フラグ112Fがセットされているとき、セキュリティコントローラからの制御により内蔵RAM104への書き込みを停止する。すなわち、プログラムの復号中、復号化されたプログラムの実行中は内蔵RAM104へデータを書き込むことはできない。

【0086】

メモリポート303は、プログラム復号実行フラグ112Fがリセットされているとき、セキュリティコントローラ111bにより内蔵RAM105へのアクセスを停止する。すなわち、バスポート110bが内部バス109と外部バス102とを接続している間は内蔵RAM105へのアクセスはできない。したがって、内蔵RAM105に書き込まれる復号化されたプログラムや復号処理の実行中のデータが外部から観測されることはない。

【0087】

次に、図4を用いて、暗号化されたプログラムを復号してプログラムD128aを生成し、プログラムD128aを実行する手順について説明する。

【0088】

図4は、第2の実施形態における暗号化されたプログラムの復号の手順を示すフローチャートである。

【0089】

まず、ステップST201において、CPU103bは復号プログラムD12

3aと暗号化されたプログラムとの内蔵RAM104への転送を行う。

【0090】

次に、その転送が終了すると、ステップST402に進んで、CPU103bはプログラム復号実行フラグ112Fをセットする。このとき、バスポート110bは内部バス109と外部バス102との分離を行う。また、メモリポート302は内蔵RAM104への書き込みを停止し、メモリポート303は内蔵105へのアクセスを許可する。

【0091】

次に、ステップST205に進んで、CPU103bは復号プログラムD123aを実行し、秘密鍵格納レジスタ107に格納された秘密鍵を用いて暗号化されたプログラムを復号してプログラムD128aを生成し、内蔵RAM105に書き込む。

【0092】

次に、ステップST206に進んで、CPU103bはプログラムD128aを実行する。

【0093】

最後に、プログラムD128aの実行が終了すると、ステップST207に進んで、プログラム復号実行フラグ112Fをリセットする。プログラム復号実行フラグ112Fがリセットされるとき、汎用レジスタコントローラ119bはセキュリティコントローラ111bからの制御により汎用レジスタ120bをリセットする。プログラム復号実行フラグ112Fがリセットされると、バスポート110bは内部バス109と外部バス102とを接続する。また、メモリポート302は、内蔵RAM104への書き込みを許可し、メモリポート303は内蔵RAM105へのアクセスを停止する。

【0094】

半導体集積回路装置301では、メモリポート302は、復号プログラムD123aを実行し、プログラムD128aを生成しているときは内蔵RAM104への書き込みを停止しているので、復号中のデータやプログラムD128aが内蔵RAM104に記憶されることはない。さらに、メモリポート303は、バス

ポート110が外部バス102と内部バス109とを接続しているときは内蔵RAM105へのアクセスを停止しているので、復号中のデータやプログラムD128aが外部に出力されることはない。

【0095】

以上のように第2の実施形態によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されことなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【0096】

(第3の実施形態)

図5は、第3の実施形態に係る半導体集積回路装置501の構成を説明するためのブロック図である。

【0097】

図5に示す半導体集積回路装置501は、図1に示した半導体集積回路装置101と比べ、メモリポート402をさらに備えた点で相違する。また、セキュリティコントローラ111cは、プログラム復号実行フラグ112Fを格納するフラグ格納部113cと、RAM初期化部502（メモリ初期化部に対応する）とを有する点で、図1に示したセキュリティコントローラ111aと相違する。なお、その他の要素は、図1に示した要素と同様の動作を行うので、その説明は繰り返さない。

【0098】

RAM初期化部502は、プログラム復号実行フラグ112Fがリセットされる直前に、内蔵RAM105上のすべての領域に”1”を書き込んでデータを消去する。これにより、内蔵RAM105に書き込まれた復号されたプログラムや復号中のデータが外部から観測できないようにする。

【0099】

次に、図6を用いて、暗号化されたプログラムを復号してプログラムD128aを生成し、プログラムD128aを実行する手順について説明する。

【0100】

図6は、第3の実施形態における暗号化されたプログラムの復号の手順を示すフローチャートである。

【0101】

まず、ステップST201において、CPU103cは復号プログラムD123aと暗号化されたプログラムとの内蔵RAM104への転送を行う。

【0102】

次に、その転送が終了すると、ステップST402に進んで、CPU103cはプログラム復号実行フラグ112Fをセットする。このとき、バスポート110cは内部バス109と外部バス102との分離を行う。また、このとき、メモリポート402は、セキュリティコントローラ111cからの制御によって内蔵RAM104への書き込みを停止する。

【0103】

次に、ステップST205に進んで、CPU103cは復号プログラムD123aを実行し、秘密鍵格納レジスタ107に格納された秘密鍵を用いて暗号化されたプログラムを復号してプログラムD128aを生成し、内蔵RAM105に書き込む。

【0104】

次に、生成されたプログラムD128aが内蔵RAM105に書き込まれると、ステップST206に進んで、CPU103cはプログラムD128aを実行する。

【0105】

次に、ステップST607に進んで、RAM初期化部502は内蔵RAM105上のすべての領域に"1"を書き込んでデータを消去する。

【0106】

最後に、内蔵RAM105上のデータが消去されると、ステップST207に進んで、プログラム復号実行フラグ112Fをリセットする。プログラム復号実行フラグ112Fがリセットされるとき、汎用レジスタコントローラ119cは、セキュリティコントローラ111cからの制御により汎用レジスタ120cを

リセットする。プログラム復号実行フラグ112Fがリセットされるとバスポート110cは内部バス109と外部バス102とを接続する。またこのとき、メモリポート402は、セキュリティコントローラ111cからの制御によって内蔵RAM104への書き込みを許可する。

【0107】

半導体集積回路装置501では、メモリポート402は、復号プログラムD123aを実行し、プログラムD128aを生成しているときは内蔵RAM104への書き込みを停止しているため、復号中のデータやプログラムD128aが内蔵RAM104に記憶されることはない。さらに、RAM初期化部502によって、バスポート110が外部バス102と内部バス109を分離状態から接続状態に変える直前に内蔵RAM105上のデータをすべて消去しているため、復号中のデータやプログラムD128aが外部に出力されることはない。

【0108】

以上のように第3の実施形態によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることがなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【0109】

(第4の実施形態)

図7は第4の実施形態に係る半導体集積回路装置701の構成を説明するためのブロック図である。

【0110】

図7に示す半導体集積回路装置701は、図1に示した半導体集積回路装置101に比べて、復号鍵アクセスポート703及び復号鍵格納レジスタ702をさらに備えている点で相違する。また、PC128dは、プログラムD728a及び暗号プログラムD728bに加え、復号鍵暗号プログラムD728c、暗号鍵D728d、及び復号鍵D728eを保持する点で、図1に示したPC128aと相違する。フラグ格納部113dは、プログラム復号実行フラグ112F及び

RAMコピーフラグ113Fに加え、復号鍵復号フラグ704Fを保持する点で、図1に示したフラグ格納部113aと相違する。フラッシュメモリ123dは、復号プログラム723aに加えて復号鍵復号プログラムD723bを保持する点で相違する。なお、その他の要素は、図1に示した要素と同様の動作を行うが、図1の場合と相違する部分を中心に説明する。

【0111】

CPU103dは、内蔵RAM104や105、またはフラッシュメモリ123d上に格納されたプログラムによって動作する。通常のプログラムを動作させるほか、暗号化された復号鍵、暗号化されたプログラムの復号や復号化されたプログラムを実行する。また、外部から入力される暗号化された復号鍵、暗号化されたプログラムや復号鍵復号プログラムD723b、復号プログラムD723aを内蔵RAM104に転送する。

【0112】

内蔵RAM104は、通常時、すなわち、復号プログラムD723a、復号鍵復号プログラムD723b、復号化されたプログラムのいずれもが実行されていないときに使用されるメモリである。暗号化された復号鍵を復号して復号鍵格納レジスタ702に保存する場合について説明する。まず、バスポート110dが外部バス102と内部バス109とを接続した状態で、CPU103dによって、暗号化された復号鍵とフラッシュメモリ123d内の復号鍵復号プログラムD723bとが、外部バス102及び内部バス109を経由して内蔵RAM104に転送される。次に、バスポート110dが外部バス102と内部バス109とを分離してから、DMA118dによって、暗号化された復号鍵と復号鍵復号プログラムD723bとが内蔵RAM104から内蔵RAM105に転送される。その後は、復号鍵復号プログラムD723bが終了するまでの間、セキュリティコントローラ111dによって、内部バス109から内蔵RAM104へのアクセスが禁止される。

【0113】

続いて、暗号化されたプログラムを復号して実行する場合について説明する。まず、バスポート110dが外部バス102と内部バス109とを接続した状態

で、CPU103dによって、暗号化されたプログラムと復号プログラムD723aとが内蔵RAM104に転送される。次に、バスポート110dが外部バス102と内部バス109とを分離してから、DMA118dによって、暗号化されたプログラムと復号プログラムD723aとが内蔵RAM104から内蔵RAM105に転送される。その後は、復号化されたプログラムの実行が終了するまでの間、セキュリティコントローラ111dによって、内部バス109から内蔵RAM104へのアクセスが禁止される。

【0114】

内蔵RAM105は、復号鍵復号プログラムD723b、復号プログラムD723a、及び復号化されたプログラムD728bの実行時に使用される。暗号化された復号鍵を復号して復号鍵格納レジスタ702に保存する場合について説明する。バスポート110dが外部バス102と内部バス109とを分離した後に、DMA118dによって、暗号化された復号鍵と復号鍵復号プログラムD723bが内蔵RAM104から内蔵RAM105に転送される。そして、暗号化された復号鍵の復号中、CPU103dは内蔵RAM105を使用してその復号を行う。また、暗号化されたプログラムを復号して実行する場合について説明する。バスポート110dが外部バス102と内部バス109とを分離した後に、暗号化されたプログラムと復号プログラムD723aが内蔵RAM104から内蔵RAM105に転送される。暗号化されたプログラムの復号中及び復号化されたプログラムの実行中、CPU103dは内蔵RAM105を使用して暗号化されたプログラムの復号及び復号化されたプログラムの実行を行う。バスポート110dが外部バス102と内部バス109とを接続しているとき、内部バス109から内蔵RAM105へのアクセスが禁止される。したがって、内蔵RAM105に一時的に記憶される復号化された復号鍵D728eや復号化されたプログラムD728a、これらの復号処理の実行途中のデータが外部から観測されることはない。

【0115】

公開鍵格納レジスタ106は、公開鍵を格納した読み出し専用のレジスタである。公開鍵は、半導体集積回路装置701の外部にあるパソコン128dに転送

され、復号鍵暗号プログラムD728cとともに復号鍵D728eを暗号化するために用いられる鍵である。暗号化された復号鍵は、復号鍵復号プログラムD723bと秘密鍵格納レジスタ107に格納された秘密鍵とを用いて復号される。

【0116】

秘密鍵格納レジスタ107は、秘密鍵を格納した読み出し専用のレジスタである。秘密鍵は、公開鍵を用いて暗号化された復号鍵を復号するときに用いられる鍵である。

【0117】

復号鍵格納レジスタ702は、復号鍵D728eを格納する書き込み及び読み出しが可能なレジスタである。復号鍵D728eは復号鍵復号プログラムD723bとともに、暗号化されたプログラムの復号に用いられる鍵である。

【0118】

秘密鍵アクセスポート108dは、復号鍵復号フラグ704FがセットされRAMコピーフラグ113Fがリセットされている間にのみ、CPU103dが秘密鍵格納レジスタ107から秘密鍵を読み出すことを可能にする。すなわち、復号鍵復号プログラムD723bが開始され、内蔵RAM104から内蔵RAM105への暗号化された復号鍵及び復号鍵復号プログラムD723bの転送が完了し、RAMコピーフラグ113Fがリセットされて、その後暗号化された復号鍵を復号している間にのみ、CPU103dが秘密鍵格納レジスタ107から秘密鍵を読み出すことを可能にし、それ以外のときは秘密鍵の読み出しを禁止する。

【0119】

復号鍵アクセスポート703は、復号鍵復号フラグ704Fがセットされ、かつRAMコピーフラグ113Fがリセットされている間は、復号鍵D728eの書き込みを可能にする。また、プログラム復号実行フラグ112Fがセットされ、かつRAMコピーフラグ113Fがリセットされている間は、復号鍵D728eを読み出すことを可能にする。それ以外のときは書き込み、読み出しをともに禁止する。すなわち、復号鍵復号プログラムD723bが開始され、内蔵RAM104から内蔵RAM105への暗号化された復号鍵と復号鍵復号プログラムD723bの転送が完了し、RAMコピーフラグ113Fがリセットされて、その後

暗号化された復号鍵を復号している間は復号鍵D728eの書き込みを可能にする。また、復号プログラムD723aが開始され、内蔵RAM104から内蔵RAM105への暗号化されたプログラムと復号プログラムD723aの転送が完了し、RAMコピーフラグ113Fがリセットされて、その後暗号化されたプログラムを復号している間は復号鍵D728eの読み出しを可能にする。

【0120】

バスポート110dは、復号鍵復号フラグ704F、プログラム復号実行フラグ112F、RAMコピーフラグ113Fの少なくとも1つがセットされているときに、内部バス109と外部バス102とを分離する。このため、復号鍵復号プログラムD723b、復号プログラムD723a、復号化されたプログラムD728aの実行中は、内部バス109及び内蔵RAM105が外部から観測されることがない。その他の場合は内部バス109と外部バス102とを接続する。

【0121】

セキュリティコントローラ111dは、復号鍵復号フラグ704F、プログラム復号実行フラグ112F、及びRAMコピーフラグ113Fを保持するフラグ格納部と、CSディスパッチャ114dと、DMA118dとを内蔵する。

【0122】

復号鍵復号フラグ704Fは、復号鍵復号プログラムD723bの開始時にCPU103からセットされ、復号鍵の復号終了時にCPU103からリセットされる。復号鍵復号プログラムD723bが開始され、内蔵RAM104から内蔵RAM105への暗号化された復号鍵と復号鍵復号プログラムD723bの転送が完了し、RAMコピーフラグ113Fがリセットされる。その後、暗号化された復号鍵を復号している間は、内蔵RAM104へのアクセスを禁止し、内蔵RAM105、秘密鍵格納レジスタ107、及び復号鍵格納レジスタ702へのアクセスを可能にする。復号鍵復号フラグ704Fがリセットされると、内蔵RAM105、秘密鍵格納レジスタ107、及び復号鍵格納レジスタ702へのアクセスが禁止される。

【0123】

プログラム復号実行フラグ112Fは、復号プログラムD723aの開始時に

CPU103dからセットされ、復号化されたプログラムの実行終了時にCPU103dからリセットされる。復号プログラムD723aが開始され、内蔵RAM104から内蔵RAM105への暗号化されたプログラムと復号プログラムD723aの転送が完了し、RAMコピーフラグ113Fがリセットされる。その後、暗号化されたプログラムを復号している間と復号化されたプログラムを実行している間は、内蔵RAM104へのアクセスを禁止し、内蔵RAM105及び復号鍵格納レジスタ702へのアクセスを可能にする。プログラム復号実行フラグ112Fがリセットされると、内蔵RAM105、秘密鍵格納レジスタ107及び復号鍵格納レジスタ702へのアクセスが禁止される。

【0124】

RAMコピーフラグ113Fは、復号鍵復号プログラムD723bまたは復号プログラムD723aの開始時にCPU103dからセットされ、内蔵RAM104から内蔵RAM105へのデータの転送終了時にCPU103dからリセットされる。

【0125】

CSディスプレイパッチャ114dは、RAMコピーフラグ113Fがセットされているとき、チップセレクト信号116S及び117Sをとともにアサートする。これにより、DMA118dによる内蔵RAM104から内蔵RAM105への暗号化された復号鍵、復号鍵復号プログラムD723b、暗号化されたプログラム、及び復号プログラムD723aの転送を可能にする。また、復号鍵復号フラグ704Fまたはプログラム復号実行フラグ112Fがセットされ、かつRAMコピーフラグ113Fがリセットされているとき、チップセレクト信号116Sをネゲートするとともにチップセレクト信号115Sをチップセレクト信号117Sとして転送する。これにより、暗号化された復号鍵の復号時、暗号化されたプログラムの復号時、及び復号化されたプログラムの実行時に内蔵RAM105へのアクセスを可能にする。いずれにもあてはまらないとき、チップセレクト信号115Sをチップセレクト信号116Sとして転送するとともにチップセレクト信号117Sをネゲートする。これにより、通常時、すなわち、復号鍵復号プログラムD723b、復号プログラムD723a、復号化されたプログラムD72

8 a のいずれもが実行されていないとき、内蔵RAM105へのアクセスを禁止する。

【0126】

DMA118 d は、RAMコピーフラグ113 F がセットされたとき、内蔵RAM104から内蔵RAM105への暗号化された復号鍵、復号鍵復号プログラムD723 b、暗号化されたプログラム、復号プログラムD723 aの転送を行い、転送が終了するとRAMコピーフラグ113 Fをリセットする。

【0127】

汎用レジスタコントローラ119 d は、復号鍵復号フラグ704 Fまたはプログラム復号実行フラグ112 F がリセットされる時汎用レジスタ120 d をリセットする。したがって、暗号化された復号鍵の復号中、暗号化されたプログラムの復号中、及び復号化されたプログラムの実行中に汎用レジスタ120 d に生成されたデータが外部から観測されることはない。

【0128】

復号鍵復号プログラムD723 b は、フラッシュメモリ123 d に保持されている。復号鍵暗号プログラムD728 c と公開鍵とによって暗号化された復号鍵を復号する際に、半導体集積回路装置701内部の内蔵RAM104を経由して内蔵RAM105に転送され、秘密鍵格納レジスタ107に格納された秘密鍵とともに暗号化された復号鍵を復号するものである。

【0129】

復号プログラムD723 a は、フラッシュメモリ123 d に保持されている。暗号プログラムD728 b と暗号鍵D728 d とによって暗号化されたプログラムを復号する際に、半導体集積回路装置701内部の内蔵RAM104を経由して内蔵RAM105に転送され、復号鍵格納レジスタ702に格納された復号鍵とともに暗号化されたプログラムを復号するものである。

【0130】

プログラムD728 a は、暗号プログラムD728 b と暗号鍵D728 d とを用いて暗号化され、ネットワーク回線127、パソコン126、USBケーブル125、USBアップストリームポート124、外部バス102を介して半導体

集積回路装置701に転送される。そして、半導体集積回路装置701内において、復号プログラムD723aと復号鍵格納レジスタ107に格納された復号鍵D728eを用いて復号されるものである。

【0131】

暗号プログラムD728bは、暗号鍵D728dを用いてプログラムD728aを暗号化するものである。

【0132】

復号鍵暗号プログラムD728cは、公開鍵格納レジスタ106に格納された公開鍵とともに復号鍵D728eを暗号化するものである。

【0133】

暗号鍵D728dは、暗号プログラムD728bとともにプログラムD728aを暗号化するものである。

【0134】

復号鍵D728eは、復号プログラムD723aとともに、暗号鍵D728を用いて暗号化されたプログラムを復号するものである。

【0135】

情報機器740は、半導体集積回路装置701、周辺機器150、フラッシュメモリ123d、USBアップストリームポート124とを有している。

【0136】

次に、図8を用いて、暗号化された復号鍵を復号して復号鍵D728eを復号鍵格納レジスタ702に格納する手順について説明する。

【0137】

図8は、第4の実施形態における暗号化された復号鍵の復号の手順を示すフローチャートである。

【0138】

まず、ステップST801において、CPU103dは復号鍵復号プログラムD723bと暗号化された復号鍵とを内蔵RAM104への転送を行う。

【0139】

次に、その転送が終了すると、ステップST802に進んで、CPU103d

は復号鍵復号フラグ704FとRAMコピーフラグ113Fとをセットする。このとき、バスポート110dは内部バス109と外部バス102との分離を行う。

【0140】

次に、その分離後、ステップST803に進んで、DMA118dは内蔵RAM104上の復号鍵復号プログラムD723bと暗号化された復号鍵との内蔵RAM105への転送を行う。

【0141】

次に、その転送が終了すると、ステップST804に進んで、CPU103dはRAMコピーフラグ113Fをリセットする。ここから、後述するステップST805が終了するまで、CSディスパッチャ114dはチップセレクト信号116Sをアサートしない。

【0142】

次に、ステップST805に進んで、CPU103dは秘密鍵格納レジスタ107に格納された秘密鍵を用いて復号鍵復号プログラムD723bを実行し、暗号化された復号鍵を復号して復号鍵D728eを生成し、復号鍵格納レジスタ702へ書き込む。

【0143】

最後に、ステップST806に進んで、復号鍵復号フラグ704Fをリセットする。復号鍵復号フラグ704Fがリセットされるとき、汎用レジスタコントローラ119dは汎用レジスタ120dをリセットする。復号鍵復号フラグ704Fがリセットされると、バスポート110dは内部バス109と外部バス102とを接続する。また、CSディスパッチャ114dはチップセレクト信号115Sをチップセレクト信号116Sとして転送し、チップセレクト信号117Sをネゲートする。

【0144】

図9は、復号鍵復号フラグ704F、プログラム復号実行フラグ112F、及びRAMコピーフラグ113Fの状態に対応するバスポート110d、秘密鍵アクセスポート108d、復号鍵アクセスポート703、チップセレクト信号11

6 S 及び 117 S の状態を示す。

【0145】

図9において、バスポート110 d、秘密鍵アクセスポート108 d、復号鍵アクセスポート703がデータの転送を可能にする場合にはオープンと表記し、そのデータの転送が可能でない場合にはクローズと表記している。また、チップセレクト信号116 S 及び 117 S としてチップセレクト信号115 S 上の信号を転送する場合、CS115と表記している。

【0146】

図9に示すように、バスポート110 dが外部バス102と内部バス109とを接続しているときは、秘密鍵格納レジスタ107及び復号鍵格納レジスタ702へのアクセスはできない。また、チップセレクト信号116 S は、復号鍵復号プログラムD723 bが実行され、復号鍵D728 eを生成しているときはアサートされない。このため、復号中のデータや秘密鍵、復号鍵D728 eが内蔵RAM104に記憶されることはない。さらに、チップセレクト信号117 S は、バスポート110 dが外部バス102と内部バス109とを接続しているときはネゲートされているので、復号中のデータや秘密鍵、復号鍵D728 eが外部に出力されることはない。

【0147】

次に、図10を用いて、暗号化されたプログラムを復号してプログラムD728 aを生成し、プログラムD728 aを実行する手順について説明する。

【0148】

図10は、第4の実施形態における暗号化されたプログラムの復号の手順を示すフローチャートである。

【0149】

まず、ステップST1001において、CPU103 dは復号プログラムD723 aと暗号化されたプログラムとを内蔵RAM104に転送する。

【0150】

次に、その転送が終了すると、ステップST1002に進んで、CPU103 dはプログラム復号実行フラグ112 F、RAMコピーフラグ113 Fをセット

する。このとき、バスポート110dは内部バス109と外部バス102との分離を行う。

【0151】

次に、その分離後、ステップST1003に進んで、DMA118dは内蔵RAM104上の復号プログラムD723aと暗号化されたプログラムとの内蔵RAM105への転送を行う。

【0152】

次に、その転送が終了すると、ステップST1004に進んで、CPU103dはRAMコピーフラグ113Fをリセットする。ここから、後述するステップST1006が終了するまで、CSデイスパッチャ114dはチップセレクト信号116Sをアサートしない。

【0153】

次に、ステップST1005に進んで、CPU103dは復号鍵D728eを用いて復号プログラムD723aを実行し、暗号化されたプログラムを復号してプログラムD728aを生成する。そして、生成されたプログラムD728aを内蔵RAM105に書き込む。

【0154】

次に、ステップST1006に進んで、CPU103dはプログラムD728aを実行する。

【0155】

最後に、ステップST1007に進んで、CPU103dはプログラム復号実行フラグ112Fをリセットする。プログラム復号実行フラグ112Fがリセットされるとき、汎用レジスタコントローラ119dは汎用レジスタ120dをリセットする。プログラム復号実行フラグ112Fがリセットされると、バスポート110dは内部バス109と外部バス102とを接続する。また、CSデイスパッチャ114dはチップセレクト信号115Sをチップセレクト信号116Sとして転送し、チップセレクト信号117Sをネゲートする。

【0156】

上記図9で示したように、チップセレクト信号116Sは、復号プログラムD

7 2 3 a を実行し、プログラム D 7 2 8 a を生成しているときはアサートされない。このため、復号中のデータや復号鍵 D 7 2 8 e、プログラム D 7 2 8 a が内蔵 RAM 1 0 4 に記憶されることはない。さらに、チップセレクト信号 1 1 7 S は、バスポート 1 1 0 d が外部バス 1 0 2 と内部バス 1 0 9 とを接続しているときはネゲートされるので、復号中のデータや復号鍵 D 7 2 8 e、プログラム D 7 2 8 a が外部に出力されることはない。

【 0 1 5 7 】

このように、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要があり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【 0 1 5 8 】

さらに、暗号化されたプログラムを転送する側で暗号プログラムや暗号強度の選択することができる。

【 0 1 5 9 】

＜プログラムの引き渡し方法及びシステム＞

図 1 1 ～図 1 7 は、プログラム引き渡しシステム及びその方法を説明するための図であって、本実施形態である第 4 の実施形態を例にして以下に説明する。

【 0 1 6 0 】

図 1 1 ～図 1 7 は、プログラムの使用者側が用いる情報機器内の半導体集積回路装置 7 0 1 （第 2 の装置に対応する）と、プログラムの開発者側が用いる P C 1 2 8 d （第 1 の装置に対応する）との間で、プログラムを暗号化し、暗号化されたプログラムを復号するまでのデータのやりとりを示している。

【 0 1 6 1 】

まず、図 1 1 に示すように、使用者側の半導体集積回路装置 7 0 1 は、公開鍵格納レジスタ 1 0 6 に格納された公開鍵 D 1 0 6 を開発者側の P C 1 2 8 d に転送する。

【 0 1 6 2 】

次に、図12に示すように、開発者側のPC128dは公開鍵D106と復号鍵暗号プログラムD728cとを用いて復号鍵D728eを暗号化し、暗号化された復号鍵1201を生成する。

【0163】

次に、図13に示すように、開発者側のPC128dは暗号化された復号鍵1201を使用者側の半導体集積回路装置701に転送する。

【0164】

次に、図14に示すように、使用者側の半導体集積回路装置701は、秘密鍵格納レジスタ107に格納された秘密鍵D107と復号鍵復号プログラムD723bとを用いて、暗号化された復号鍵1201を復号し、復号鍵D728eを復号鍵格納レジスタ702に格納する。

【0165】

次に、図15に示すように、開発者側のPC128dは暗号鍵D728dと暗号プログラムD728bとを用いてプログラムD728aを暗号化し、暗号化されたプログラム1501を生成する。

【0166】

次に、図16に示すように、開発者側のPC128dは暗号化されたプログラム1501を使用者側の半導体集積回路装置701に転送する。

【0167】

最後に、図17に示すように、使用者側の半導体集積回路装置701は、暗号化されたプログラム1501を復号鍵D728eと復号プログラムD723aとを用いて復号し、そして、復号化されたプログラムD728aを実行する。

【0168】

このようにすることで、暗号化されたプログラムは、プログラム開発者側の所有する暗号鍵により暗号化されて使用者側に渡され、プログラム開発者側の所有する復号鍵により復号化することができるので、プログラム開発者側の所望する暗号強度によりプログラムを暗号化して渡すことが可能になる。

【0169】

なお、以上で説明した第1～第4の実施形態における半導体集積回路では、内

蔵RAM104、内蔵RAM105の制御をチップセレクト信号を用いて行う場合について説明したが、ライトイネーブル信号・リードイネーブル信号を用いた場合であっても、同様に、各実施形態において本発明は実施可能であることは言うまでもない。

【0170】

【発明の効果】

以上のように、本発明に係る半導体集積回路装置によると、復号プログラムを保持するための不揮発性のメモリを半導体集積回路装置の内部に備える必要がなくなり、コストを低減することができる。また、復号中のプログラム及びデータを外部から観測されることなく、暗号化されたプログラムを復号し実行することができ、暗号化されたプログラムがハッキングされる可能性を低減できる。

【図面の簡単な説明】

【図1】 第1の実施形態における半導体集積回路装置の構成を説明するためのブロック図である。

【図2】 暗号化されたプログラムの復号の手順を示すフローチャートである。

【図3】 第2の実施形態における半導体集積回路装置の構成を説明するためのブロック図である。

【図4】 暗号化されたプログラムの復号の手順を示すフローチャートである。

【図5】 第3の実施形態における半導体集積回路装置の構成を説明するためのブロック図である。

【図6】 暗号化されたプログラムの復号の手順を示すフローチャートである。

【図7】 第4の実施形態における半導体集積回路装置の構成を説明するためのブロック図である。

【図8】 暗号化された復号鍵の復号の手順を示すフローチャートである。

【図9】 フラグの状態、バスポート、及びチップセレクト信号の状態の相関を示す図である。

【図 1 0】 暗号化されたプログラムの復号の手順を示すフロチャートである。

【図 1 1】 使用者側からプログラム開発者側への公開鍵の転送を示す図である。

【図 1 2】 復号鍵の暗号化を示す図である。

【図 1 3】 プログラム開発者側から使用者側への暗号化された復号鍵の転送を示す図である。

【図 1 4】 暗号化された復号鍵の復号を示す図である。

【図 1 5】 プログラムの暗号化を示す図である。

【図 1 6】 プログラム開発者側から使用者側への暗号化されたプログラムの転送を示す図である。

【図 1 7】 暗号化されたプログラムの復号を示す図である。

【図 1 8】 従来の半導体集積回路装置の構成を示すブロック図である。

【符号の説明】

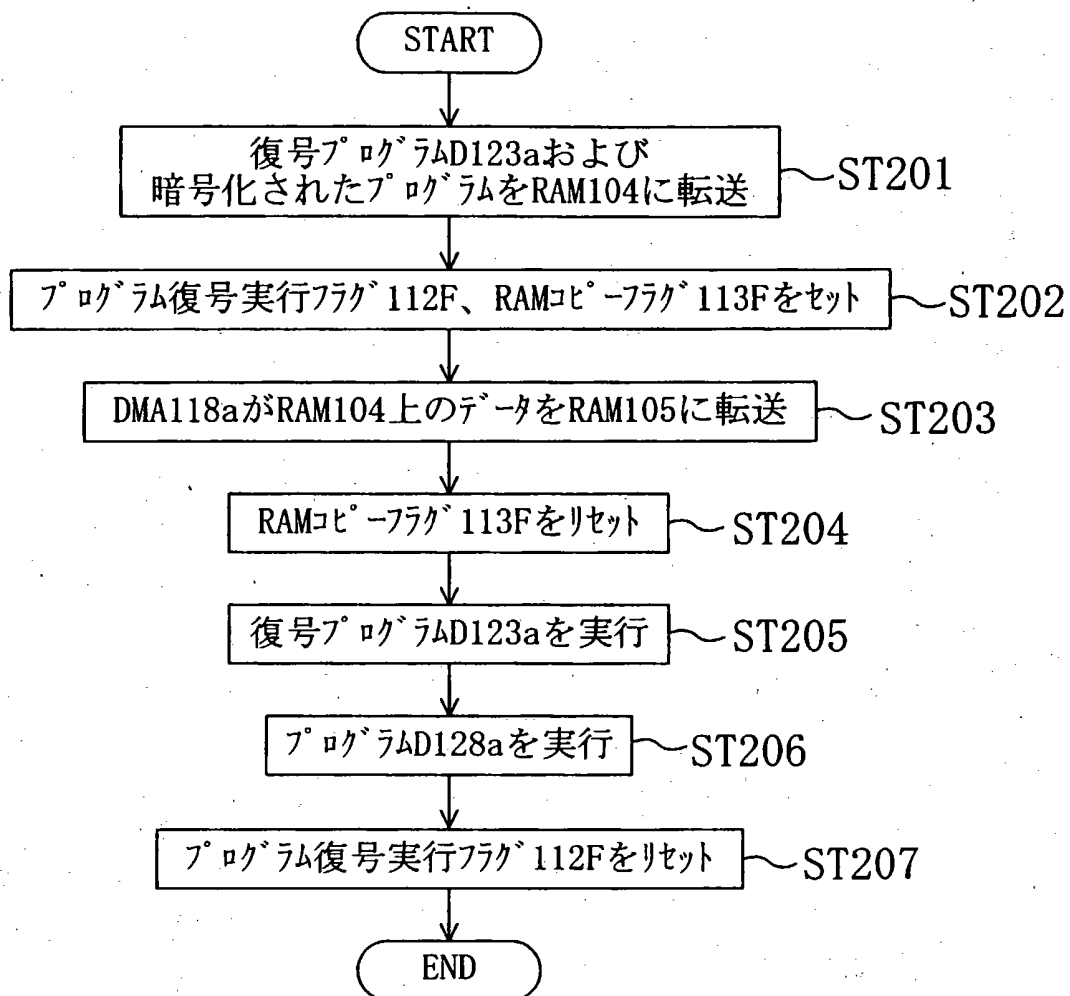
- 1 0 1 半導体集積回路（第 2 の装置）
- 3 0 1、4 0 1 半導体集積回路
- 7 0 1 半導体集積回路装置（第 2 の装置）
- 1 0 2 外部バス
- 1 0 3 a ～ 1 0 3 d CPU
- 1 0 4 内蔵 RAM（第 1 のメモリ）
- 1 0 5 内蔵 RAM（第 2 のメモリ）
- 1 0 6 公開鍵格納レジスタ
- 1 0 7 秘密鍵格納レジスタ
- 1 0 8 a、1 0 8 d 秘密鍵アクセスポート
- 1 0 9 内部バス
- 1 1 0 a ～ 1 1 0 d バスポート
- 1 1 1 a ～ 1 1 1 d セキュリティコントローラ
- 1 1 3 a、1 1 3 d フラグ格納部
- 1 1 4 a、1 0 4 d チップセレクトディスパッチャ

115S~117S チップセレクト信号
118a、118d DMAコントローラ
119a~119d 汎用レジスタコントローラ
120a~120d 汎用レジスタ
121 IOバス
122 IOポート
123a、123d フラッシュメモリ
124 USBアップストリームポート
125 USBケーブル
126 パソコン
127 ネットワーク回線
128a、128d パソコン（第1の装置）
140、740 情報機器
150 周辺機器
151 サウンドモジュール
152 ビデオモジュール
302 メモリポート（第1のメモリポート）
303 メモリポート（第2のメモリポート）
502 RAM初期化部（メモリ初期化部）
702 復号鍵格納レジスタ
703 復号鍵アクセスポート
D123a 復号プログラム
D123b 復号鍵復号プログラム
D128a、D728a プログラム
D128b、D728b 暗号プログラム
D128c、D728c 復号鍵暗号プログラム
D728d 暗号鍵
D728e 復号鍵
112F プログラム復号実行フラグ（第2のフラグ）

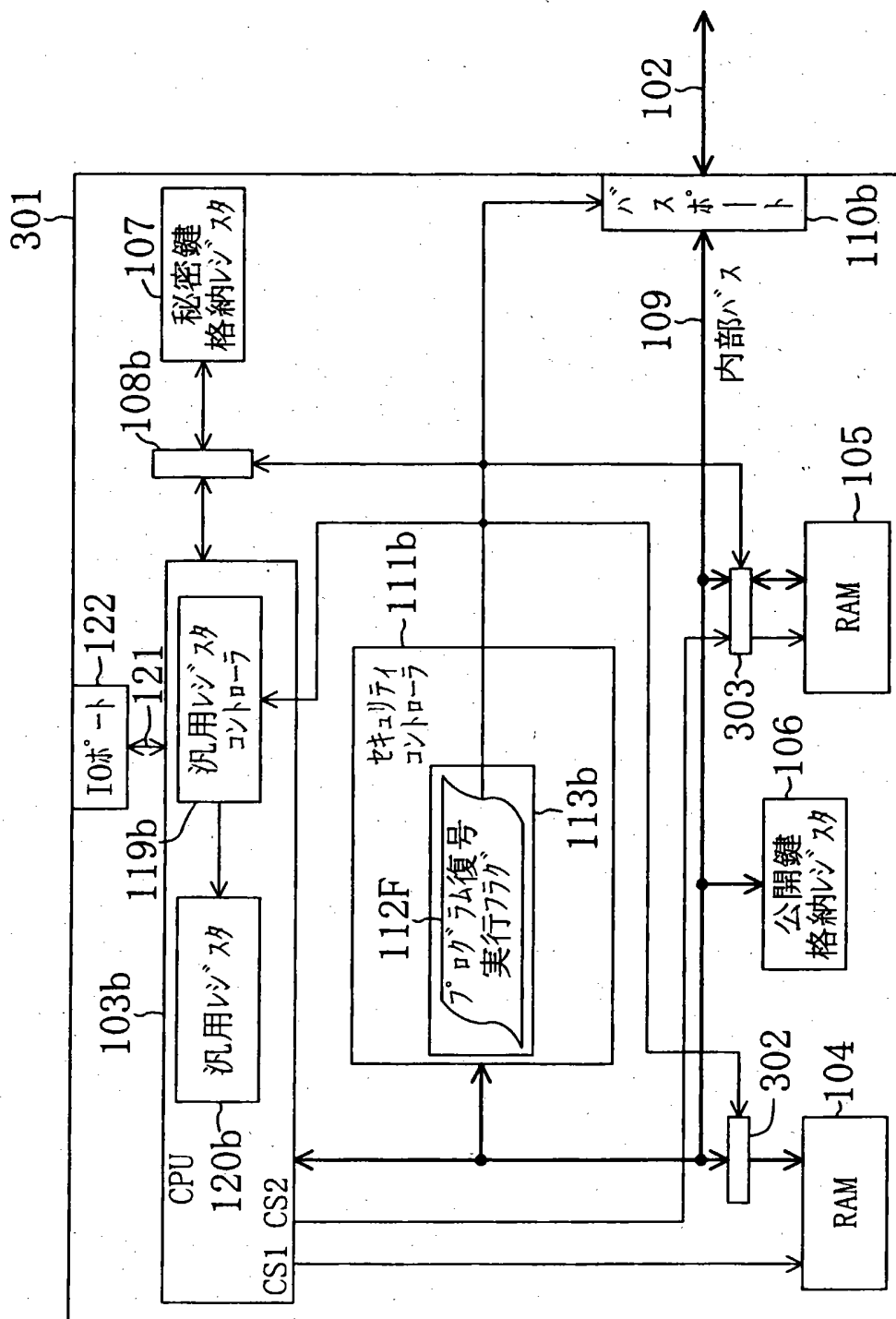
113F RAMコピーフラグ(第1のフラグ)

704F 復号鍵復号フラグ

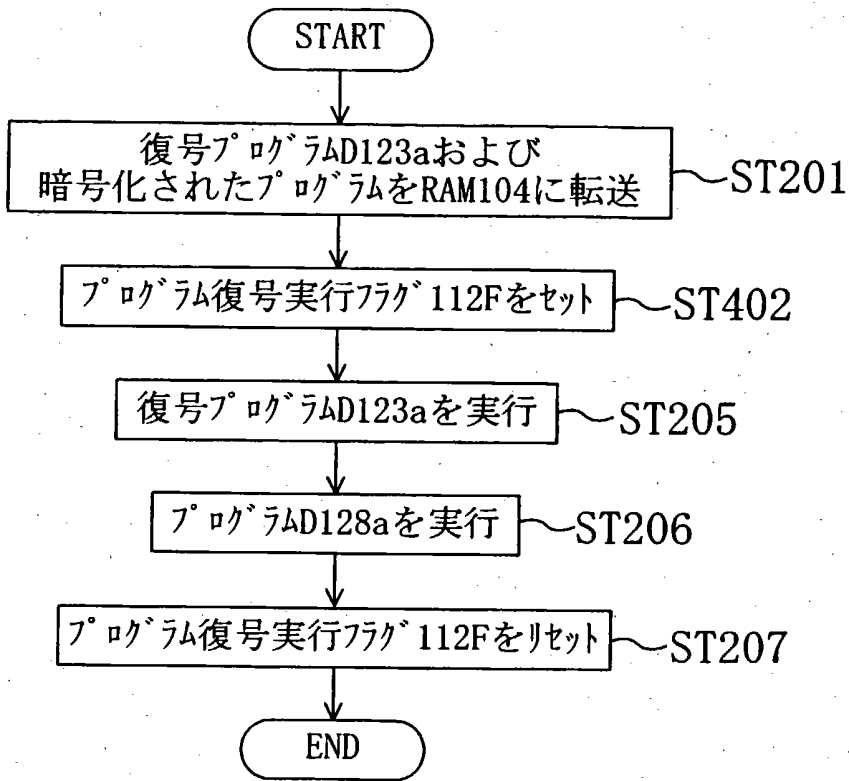
【図2】



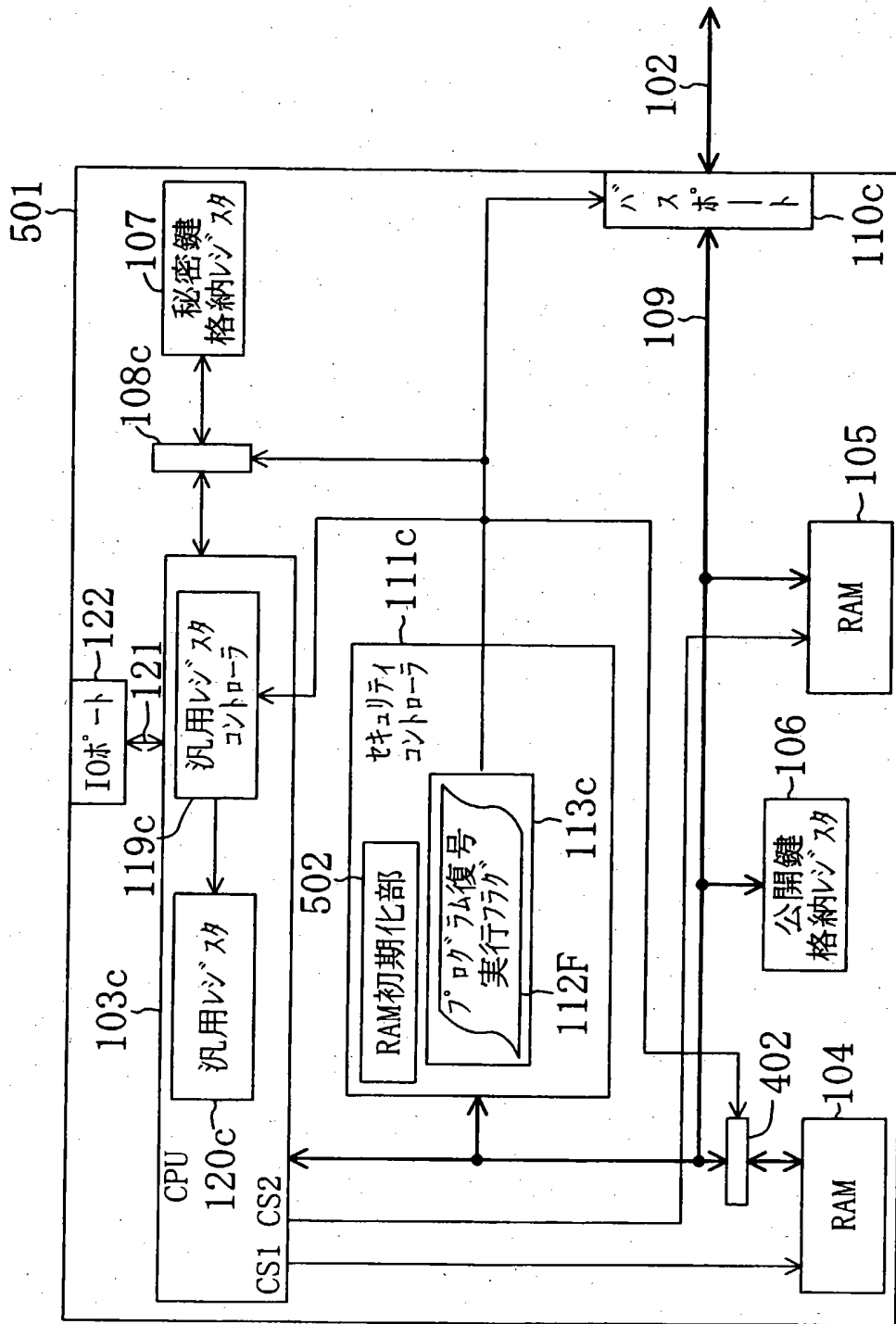
【図 3】



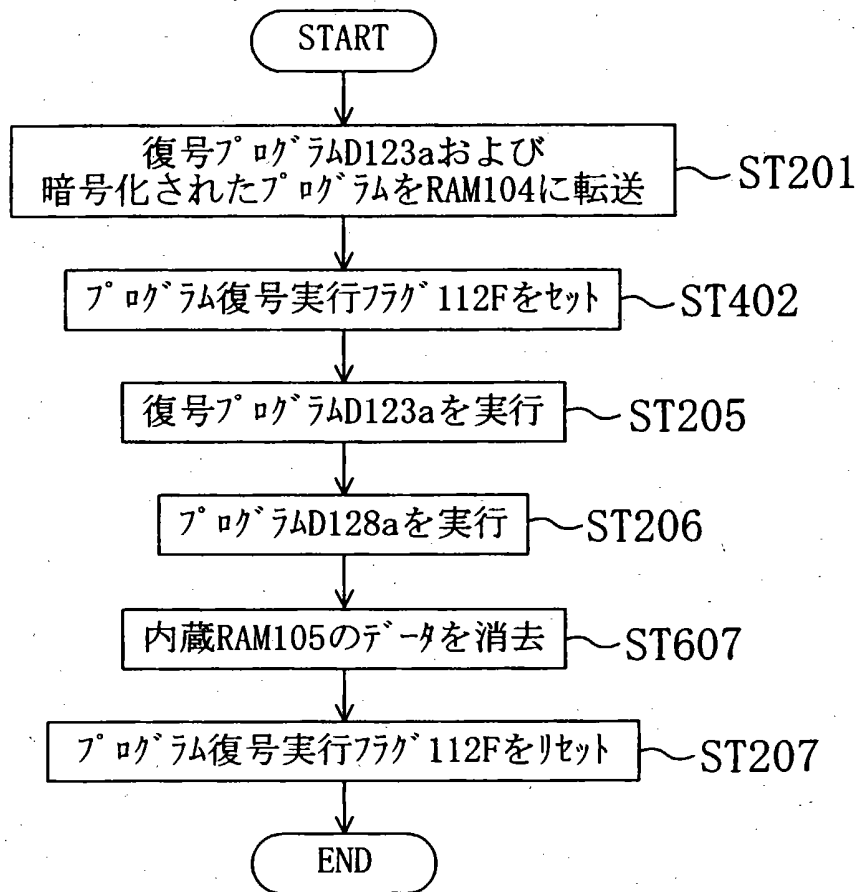
【図4】



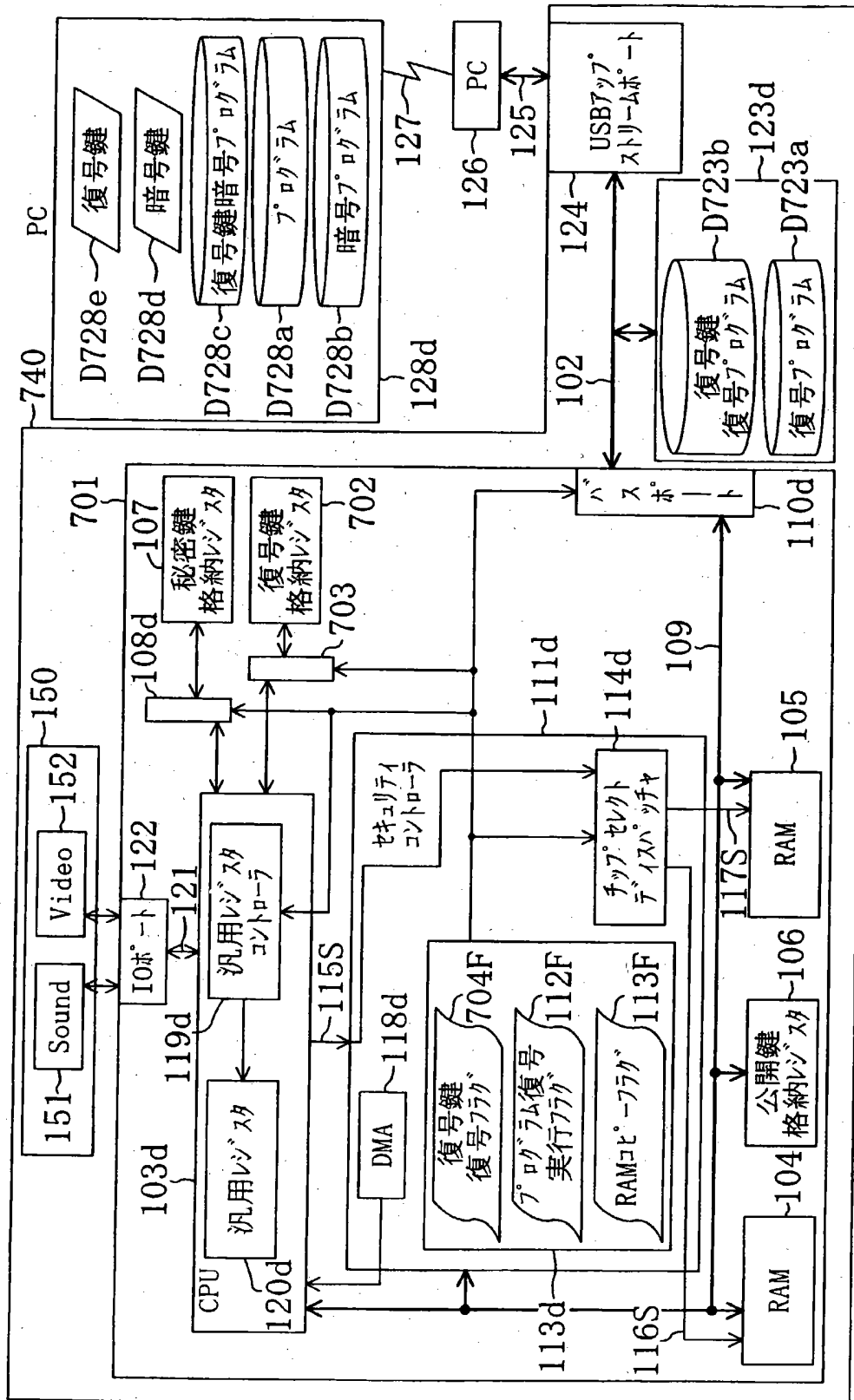
【図 5】



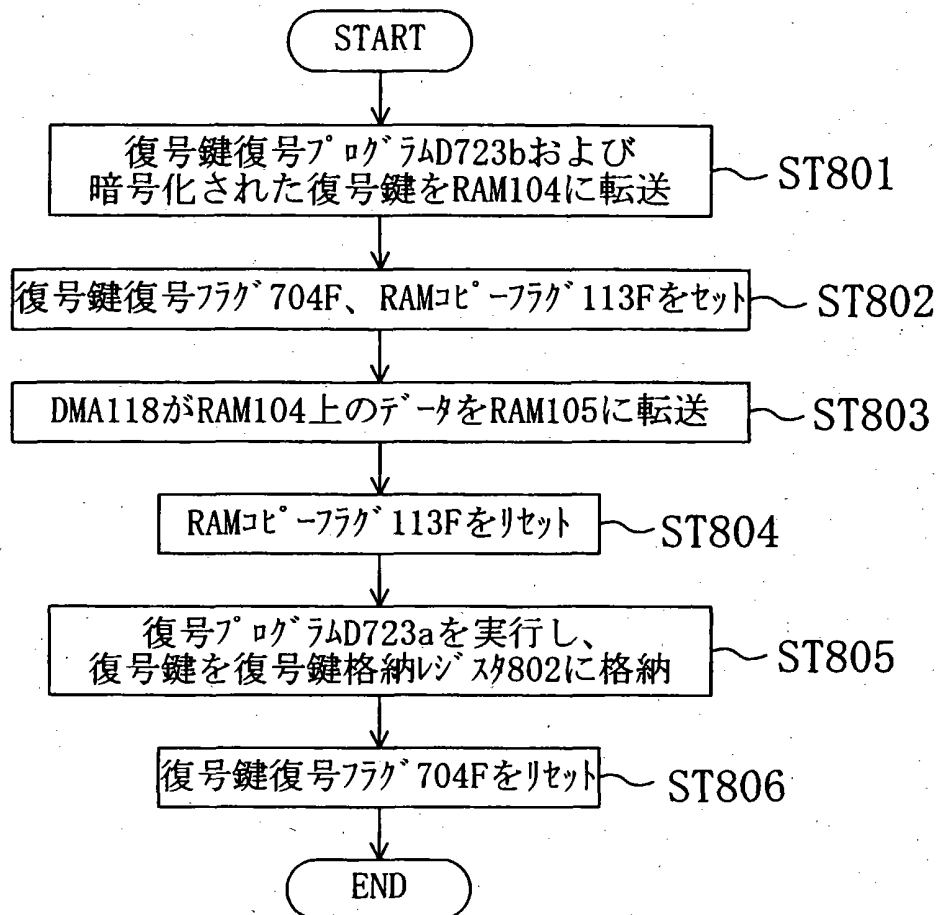
【図6】



【图 7】



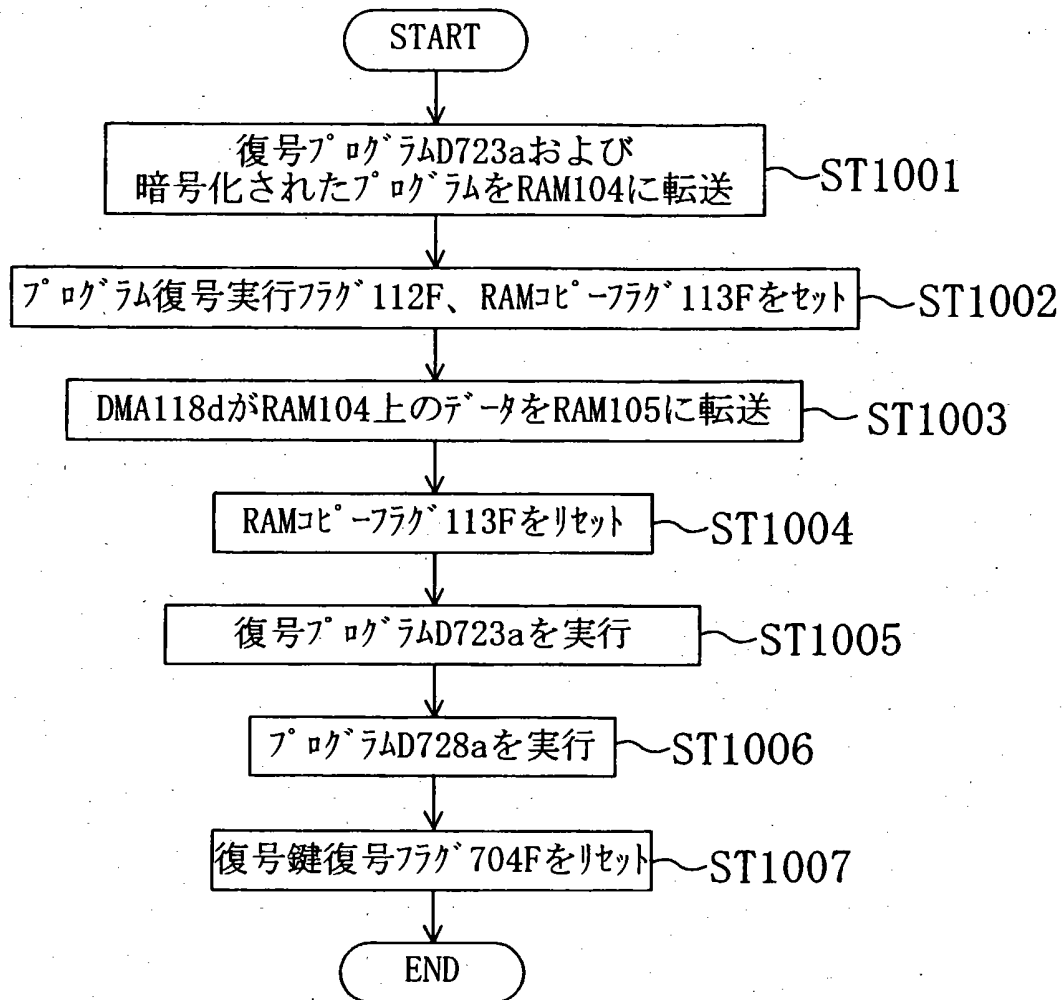
【図 8】



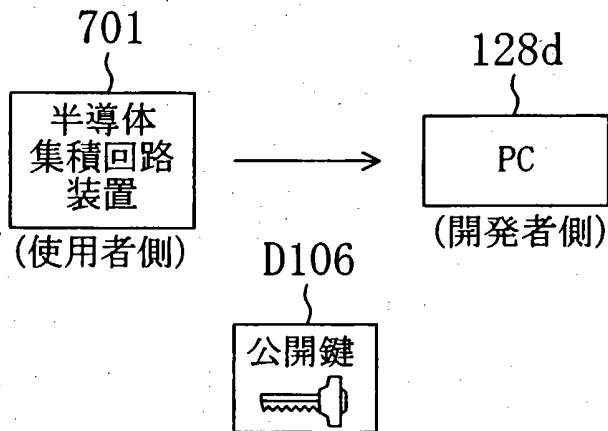
【図 9】

RAMコピ-フラグ 113F	0	1	0	1	0
復号鍵復号フラグ 704F	0	1	1	0	0
プログラム復号実行フラグ 112F	0	0	0	1	1
バスポート110d	オープン	クローズ	クローズ	クローズ	クローズ
秘密鍵アクセスポート108d	クローズ	クローズ	オープン	クローズ	クローズ
復号鍵アクセスポート703	クローズ	クローズ	オープン	クローズ	オープン
チップセレクト信号116S	CS115	アサート	ネゲ-ート	アサート	ネゲ-ート
チップセレクト信号117S	ネゲ-ート	アサート	CS115	アサート	CS115

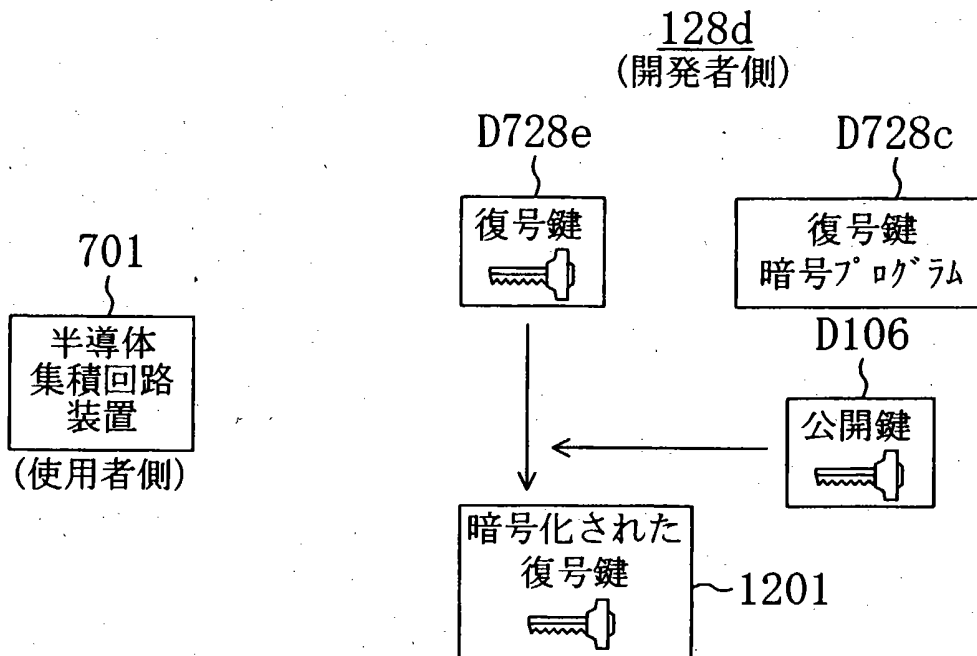
【図10】



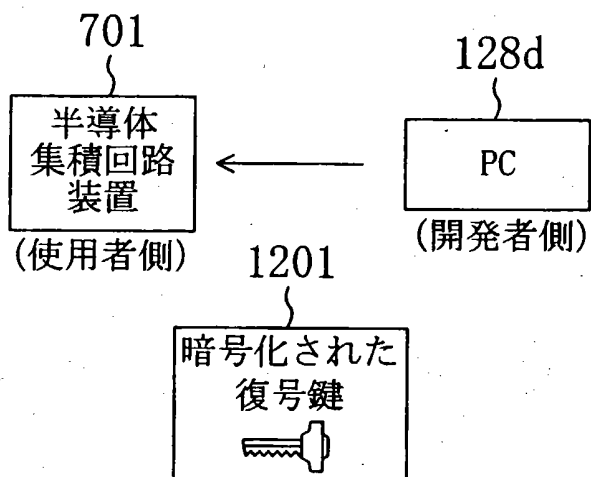
【図11】



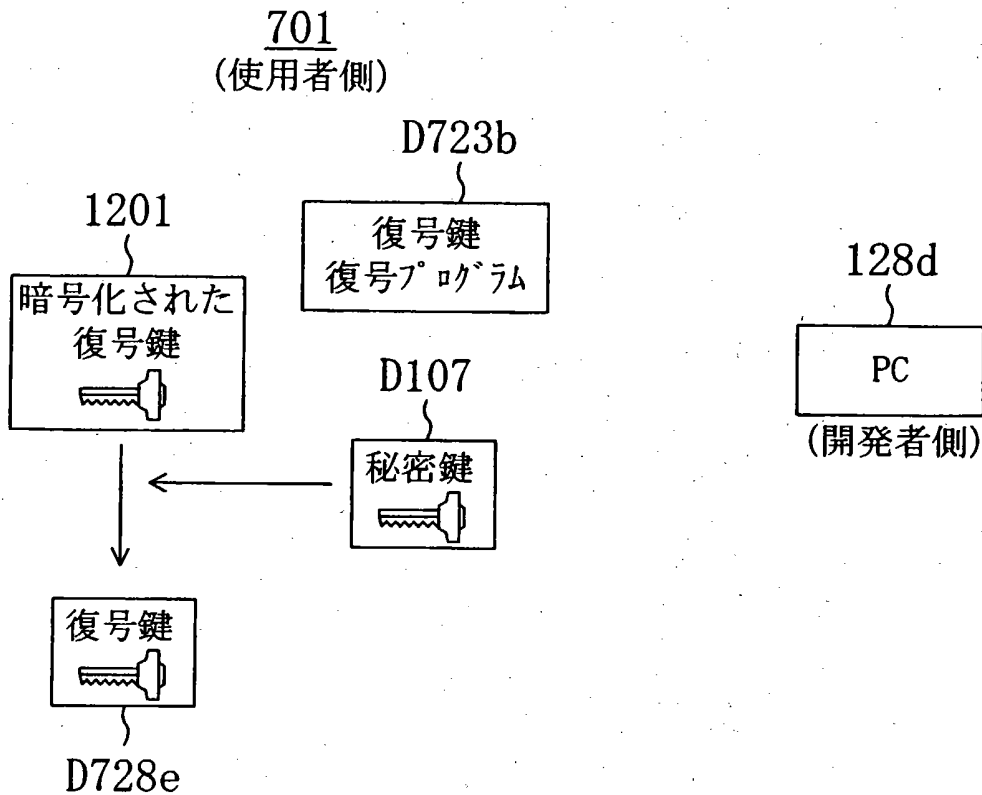
【図 12】



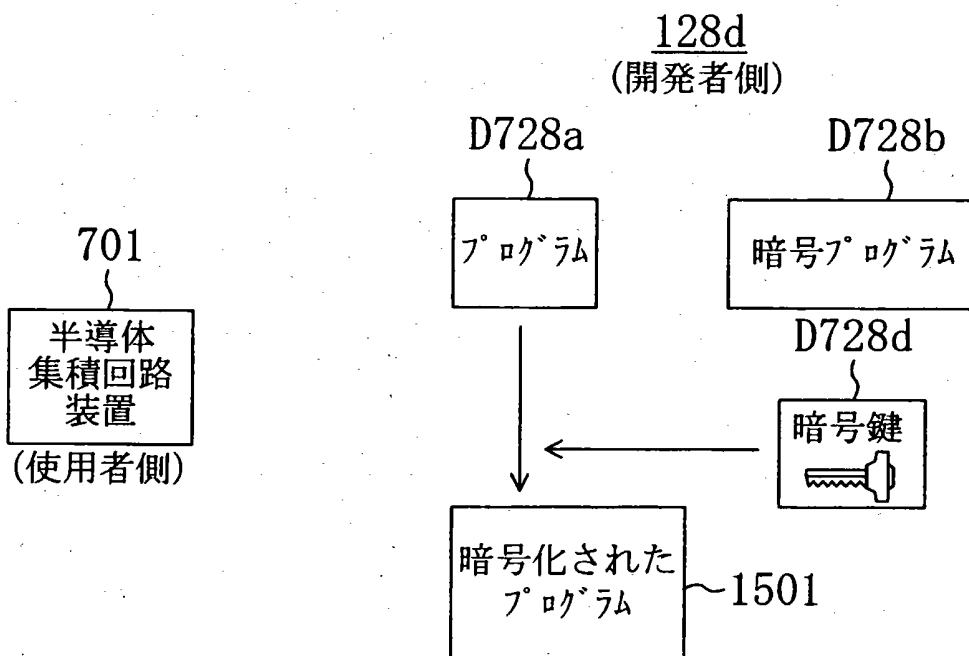
【図 13】



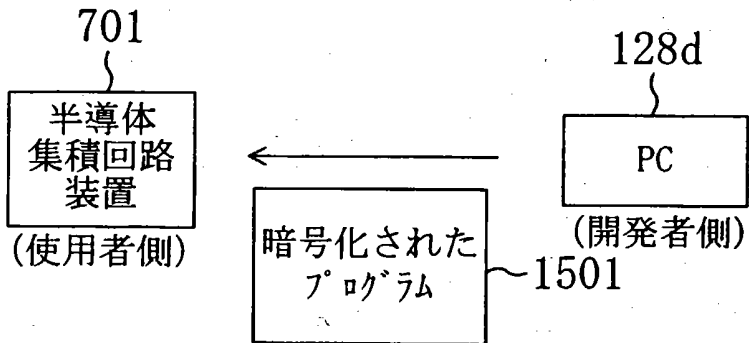
【図14】



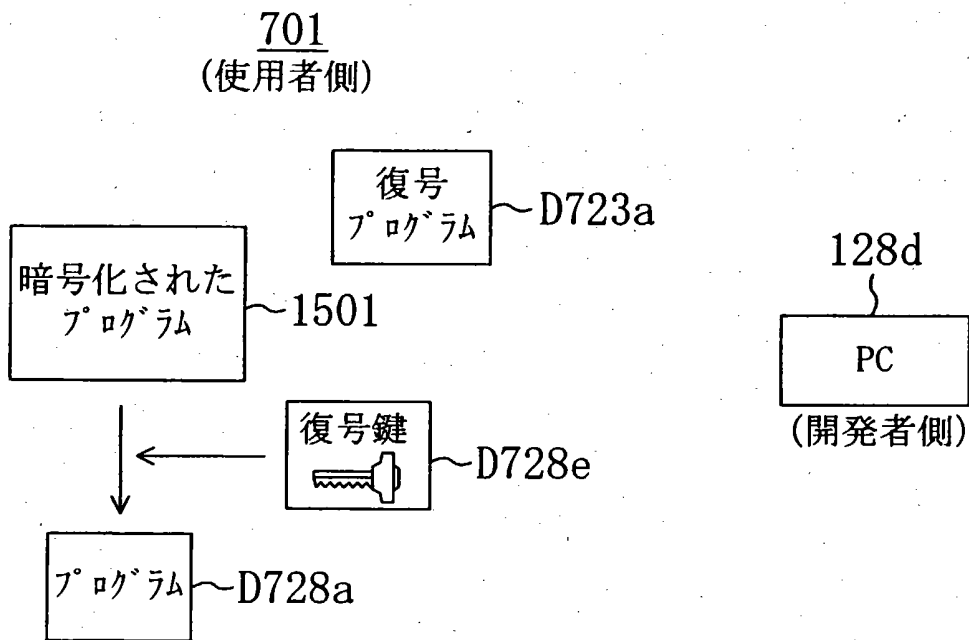
【図15】



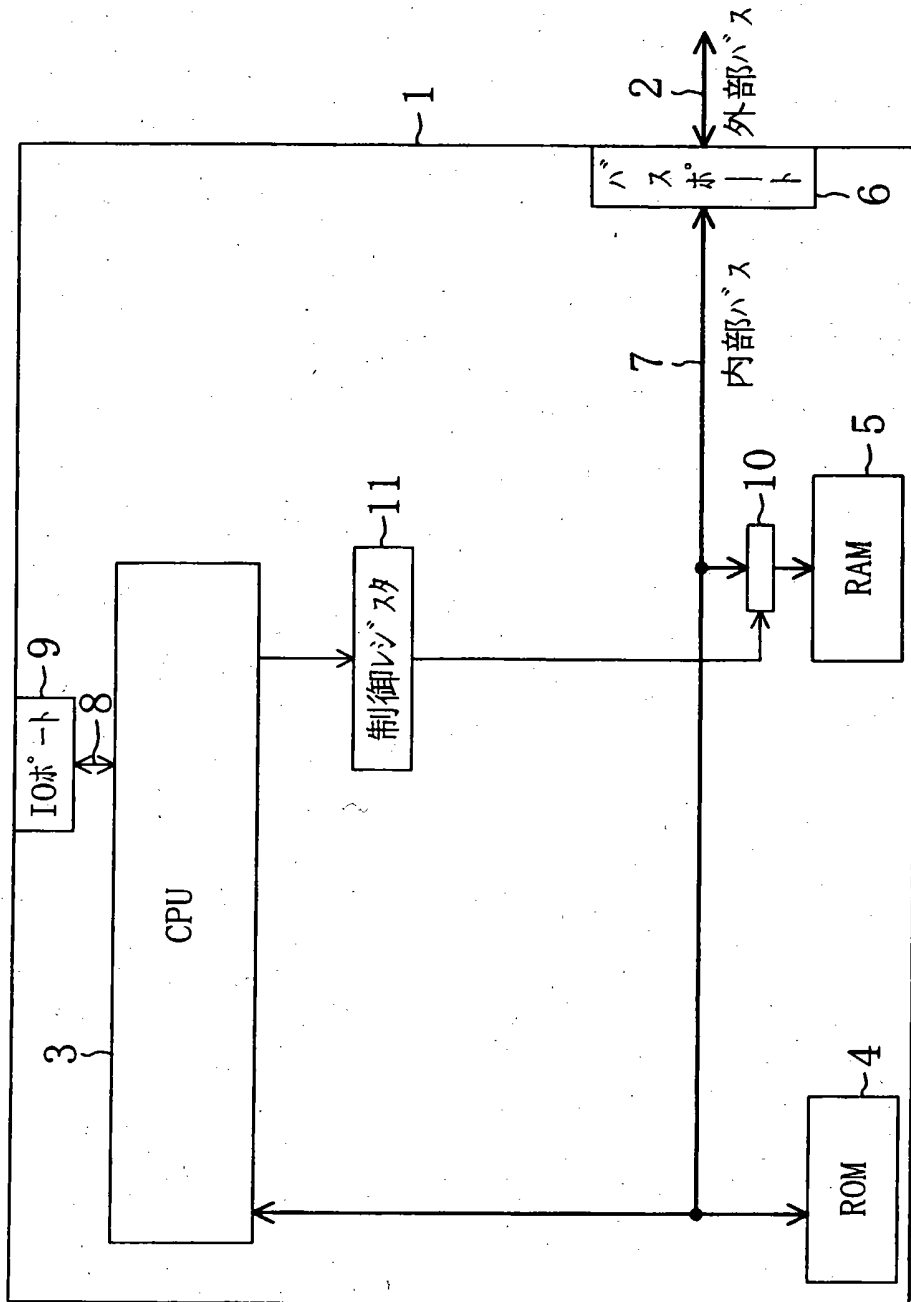
【図 16】



【図 17】



【図18】



【書類名】 要約書

【要約】

【課題】 復号プログラムを保持する不揮発性メモリを搭載不要とし、また、復号化されたプログラムを外部から観測されることなく、暗号化されたプログラムを復号・実行する半導体集積回路装置を提供する。

【解決手段】 本発明の半導体集積回路装置 1 0 1 は、暗号化されたプログラムと復号プログラム D 1 2 3 a とが R A M 1 0 5 に入力されると、バスポート 1 1 0 a に対して外部からのアクセスを禁止させ、R A M 1 0 4 及び 1 0 5 へのアクセスを許可して暗号化されたプログラムと復号プログラムとの R A M 1 0 5 への転送を行う。そして、その転送が終了すると R A M 1 0 4 へのアクセスを禁止し、C P U 1 0 3 a に対して秘密鍵保持部 1 0 7 に保持された秘密鍵と復号プログラム D 1 2 3 a とを用いた暗号化されたプログラムの復号とその復号化されたプログラムの実行を命じる。その実行終了後に R A M 1 0 5 へのアクセスを禁止する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社